

DROITS HUMAINS ET INTELLIGENCE ARTIFICIELLE



**MANUEL DU COMITÉ DIRECTEUR
POUR LES DROITS HUMAINS (CDDH)**

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

MANUEL SUR LES DROITS HUMAINS ET L'INTELLIGENCE ARTIFICIELLE

**MANUEL DU COMITÉ DIRECTEUR
POUR LES DROITS HUMAINS (CDDH)**

**Édition anglaise :
HANDBOOK ON HUMAN RIGHTS AND
ARTIFICIAL INTELLIGENCE**

Toute demande de reproduction ou de traduction de tout ou d'une partie de ce document doit être adressée à la Direction Générale Droits humains et État de droit (F 67075 Strasbourg Cedex).

Toute autre correspondance relative à ce document doit être adressée à la Division de la Coopération intergouvernementale en matière de droits humains.

Mise en page : SPDP, Conseil de l'Europe
© Conseil de l'Europe, avril 2026
Imprimé dans les ateliers du Conseil de l'Europe



Table des matières

1. INTRODUCTION	6
2. SYSTÈMES D'IA : CONCEPTS TECHNIQUES CLÉS PERTINENTS POUR LES DROITS HUMAINS	8
2.1 Système d'intelligence artificielle	8
2.1.1 Cycle de vie des systèmes d'IA	9
2.1.2 Un système basé sur des machines	9
2.1.3 L'autonomie	10
2.1.4 La capacité d'adaptation	10
2.1.5 Les objectifs du système d'IA.....	10
2.1.6 L'environnement ou le contexte	11
2.1.7 Les données d'entrée	11
2.1.8 L'inférence.....	11
2.1.9 Les données de sortie	12
2.2 Autres concepts techniques pertinents pour l'IA et les droits humains	12
2.2.1 La transparence	12
2.2.2 L'explicabilité	13
2.2.3 L'interprétabilité	14
3. DROITS HUMAINS ET INTELLIGENCE ARTIFICIELLE	15
3.1 Questions générales	15
3.1.1 La Convention européenne des droits de l'homme (CEDH)....	15
3.1.2 La Charte sociale européenne (CSE).....	15
3.1.3 La Convention-cadre sur l'intelligence artificielle et les droits de l'homme, la démocratie et l'État de droit.....	16
3.1.4 Les principes généraux de la CEDH et de la CSE dans le contexte de l'IA	18
Protection effective des droits	18
Subsidiarité et la marge d'appréciation	19
Interprétation évolutive et doctrine de « l'instrument vivant » ..	20
Obligations positives	20
Dignité humaine	22
Autonomie personnelle et autodétermination	22
Légalité, but légitime, nécessité, proportionnalité et juste équilibre	23
3.1.5 Principales questions relatives aux droits humains dans les secteurs de la gouvernance publique	24
Non-discrimination et égalité	24
i. L'interdiction de la discrimination	24
ii. Risques pour la non-discrimination et l'égalité.....	25

Le droit à la vie privée et à la protection des données à caractère personnel	27
i. Le droit à la vie privée et à la protection des données dans la CEDH et dans d'autres instruments pertinents	27
ii. Risques liés à la protection de la vie privée et des données	29
Des recours effectifs	29
i. Le droit à un recours effectif dans la CEDH, la CSE et autres instruments pertinents.....	29
ii. Risques pour le droit à un recours effectif	31
3.2 Entreprises et droits humains	31
3.2.1 Obligations positives en vertu de la CEDH et de la CSE	32
Obligations de réglementer et de surveiller les activités des entreprises.....	34
Obligations procédurales positives pour permettre la participation du public et une prise de décision en connaissance de cause.....	35
Obligations relatives à la mise en place de voies de recours effectives	37
Marge d'appréciation dans le cadre des obligations positives	37
3.2.2 Équilibrer les droits des entreprises dans le contexte de la gouvernance de l'IA.....	37
3.2.3 Principaux cadres non contraignants sur les entreprises, les droits humains et l'IA	39
Instruments non contraignants pertinents.....	39
Responsabilité des entreprises en matière de respect des droits humains	39
4. ANALYSE SECTORIELLE DE LA GOUVERNANCE PUBLIQUE	41
4.1. Administration de la justice	42
Principaux cas d'utilisation de l'IA	42
Droits humains et principes pertinents	44
Vie privée et protection des données dans le cadre de l'administration de la justice	49
4.2. Application de la loi et la sécurité publique.....	51
Principaux cas d'utilisation de l'IA	52
Droits humains et principes pertinents	52
Vie privée et protection des données ; liberté d'expression et liberté de réunion et d'association.....	53
Non-discrimination et égalité.....	58
Droit à un recours effectif	59
4.3. Immigration et contrôle des frontières	60
Principaux cas d'utilisation de l'IA	61
Droits humains et principes pertinents	62

Droit à la vie privée et à la protection des données	63
Non-discrimination	65
Droit à un recours effectif	65
4.4. Processus démocratiques	67
Principaux cas d'utilisation de l'IA	68
Droits humains et principes pertinents	69
Non-discrimination et égalité	75
Transparence et responsabilité	75
Droit à la vie privée et à la protection des données	76
Entreprises et droits humains.....	77
4.5. Soins de santé	79
Principaux cas d'utilisation de l'IA	79
Droits humains et principes pertinents	80
Droit à la vie privée et à la protection des données	82
Non-discrimination et accès équitable aux soins de santé	83
Consentement éclairé, autonomie et prise de décision	84
4.6. Services sociaux et protection sociale	86
Principaux cas d'utilisation de l'IA	87
Droits humains et principes pertinents	87
Droit à la vie privée et à la protection des données	89
Non-discrimination et égalité	90
Transparence et responsabilité	91
Accessibilité et qualité des soins	92
4.7. L'éducation.....	94
Principaux cas d'utilisation de l'IA	94
Droits humains et principes pertinents	95
Droit à la vie privée et à la protection des données	96
Non-discrimination et égalité	98
Transparence et responsabilité	101
Entreprises et droits humains.....	102
4.8. Travail et emploi	104
Principaux cas d'utilisation de l'IA	104
Droits humains et principes pertinents	105
Droit à la vie privée et à la protection des données	106
Non-discrimination et égalité	108
Transparence et responsabilité	110
Liberté d'expression ; liberté de réunion et d'association	110

1. INTRODUCTION

1. L'intelligence artificielle (IA) influe de plus en plus sur divers aspects de la société, ouvrant de nouvelles perspectives d'innovation et de progrès. Elle peut notamment faire progresser les droits humains, par exemple en accélérant les procédures judiciaires, en améliorant les soins de santé grâce à des diagnostics prédictifs et en personnalisant l'éducation pour répondre aux besoins d'apprentissage individuels. Cependant, ces opportunités s'accompagnent de risques pour les droits humains.

2. La menace potentielle que représentent le développement et l'utilisation des systèmes d'IA pour les droits humains a été reconnue par la communauté internationale et a déclenché des efforts mondiaux pour réglementer cet ensemble de technologies¹. Le Conseil de l'Europe a commencé à travailler sur le thème de l'IA il y a dix ans et a intensifié ses efforts ces dernières années, plusieurs organes et comités du Conseil de l'Europe ayant publié un certain nombre de documents politiques, de recommandations, de déclarations, de lignes directrices et d'autres instruments juridiques². La Convention-cadre du Conseil de l'Europe sur l'intelligence artificielle et les droits de l'homme, la démocratie et l'État de droit (« la Convention-cadre ») est le premier traité international sur l'IA et les droits humains³. Elle établit des principes et des obligations visant à garantir que les systèmes d'IA soient pleinement conformes aux droits humains, à la démocratie et à l'État de droit tout au long de leur cycle de vie, tout en étant propices au progrès technologique et à l'innovation⁴.

3. Les instruments existants du Conseil de l'Europe en matière de droits humains, tels que la Convention européenne des droits de l'homme et ses protocoles (CEDH) et la Charte sociale européenne (CSE), restent

¹ Voir par exemple le règlement (UE) 2024/1689 du Parlement européen et du Conseil (« Loi sur l'IA ») de l'Union européenne ; la « Recommandation sur l'intelligence artificielle » de l'OCDE adoptée en 2019, révisée en 2023 et 2024 ; la « Recommandation sur l'éthique de l'intelligence artificielle » de l'UNESCO, adoptée en 2021. La résolution A/RES/78/265 de l'Assemblée générale des Nations Unies « Saisir les opportunités offertes par des systèmes d'intelligence artificielle sûrs, sécurisés et dignes de confiance pour le développement durable » (21 mars 2024) ; et la résolution A/RES/78/311 « Intensifier la coopération internationale en matière de renforcement des capacités dans le domaine de l'intelligence artificielle » (1^{er} juillet 2024).

² Pour un aperçu des travaux réalisés jusqu'à présent, ou prévus, par les comités intergouvernementaux et autres entités du Conseil de l'Europe dans le domaine de l'IA, voir Le Conseil de l'Europe et l'intelligence artificielle.

³ État des signatures et des ratifications au 16/01/2025 - <https://www.coe.int/fr/web/conventions/full-list?module=signatures-by-treaty&treatynum=225>.

⁴ Article 1 – Objet et but, paragraphe 1.

applicables dans le contexte de l'IA : les États membres doivent aligner leurs cadres réglementaires en matière d'IA sur leurs obligations au titre de la CEDH et de la CSE. Ces instruments, interprétés respectivement par la Cour européenne des droits de l'homme (« la Cour ») et le Comité européen des droits sociaux (CEDS), établissent des normes de base pour la protection des droits humains, y compris dans des domaines qui ne sont pas couverts par la Convention-cadre, ainsi que pour les États membres qui ne sont pas parties à la Convention-cadre.⁵

4. Ce Manuel sur les droits humains et l'intelligence artificielle (« le Manuel ») a été conçu comme un outil accessible destiné principalement à aider les fonctionnaires et les responsables politiques des États membres du Conseil de l'Europe à appliquer les normes de la CEDH, de la CSE et d'autres normes pertinentes aux défis liés à l'IA. Compte tenu de la diversité de l'audience des décideurs politiques et des fonctionnaires travaillant dans divers domaines de la gouvernance publique, ce Manuel ne présume pas d'une connaissance préalable approfondie de la législation relative aux droits humains ou des questions liées à l'IA. Il ne vise pas non plus à fournir une analyse exhaustive de chaque sujet abordé. En tant que ressource pratique, il donne un aperçu de la manière dont ces normes, ainsi que des instruments tels que la Convention-cadre, peuvent s'appliquer aux activités du cycle de vie des systèmes d'IA. En se concentrant sur les principaux cas d'utilisation de l'IA dans la gouvernance publique, tant actuels que raisonnablement prévisibles, il propose un cadre permettant d'évaluer les impacts de l'IA sur les droits humains en tenant compte des normes de la CEDH et du CES, sans prédire les résultats spécifiques de cas futurs.⁶

5. La partie 2 du Manuel présente des concepts clés techniques liant les aspects technologiques de l'IA aux implications en matière de droits humains. La partie 3 expose les principes généraux des droits humains au titre de la CEDH et de la CSE applicables à l'IA dans certains secteurs publics. Il aborde tout d'abord les questions transversales pertinentes pour tous les secteurs. Il fournit ensuite une analyse sectorielle des cas d'utilisation de l'IA dans la gouvernance publique, en examinant les impacts sur les droits humains, les principes juridiques pertinents et les bonnes pratiques des États membres du Conseil de l'Europe. Le Manuel examine également le rôle des entreprises dans la gouvernance de l'IA et l'application des normes relatives aux droits humains dans ce contexte. La partie 4 présente ensuite une analyse sectorielle des principaux cas

⁵ Voir ci-dessous, section 3.1.3.

⁶ Celles-ci seront fondées sur leurs circonstances factuelles spécifiques, à la lumière de la législation et de la pratique internes pertinentes de l'État membre concerné, et dans le cadre des normes européennes pertinentes qui existeront au moment de l'examen de l'affaire, voir *Zavodnik c. Slovénie*, n° 53723/13, 21 mai 2015, paragraphe 74.

d'utilisation de l'IA dans la gouvernance publique, en examinant les incidences sur les droits humains, les principes juridiques pertinents et les bonnes pratiques des États membres du Conseil de l'Europe.

2. SYSTÈMES D'IA : CONCEPTS TECHNIQUES CLÉS PERTINENTS POUR LES DROITS HUMAINS

6. Cette partie fournit une définition pratique des « systèmes d'intelligence artificielle », avec une explication de leurs fonctions de base, et identifie d'autres concepts techniques pertinents dans le contexte de ce Manuel. Les définitions fournies ci-dessous s'appuient sur diverses sources⁷. Elles ne sont ni exhaustives ni universelles⁸.

2.1 Système d'intelligence artificielle

7. « Système d'intelligence artificielle » : un système basé sur une machine qui, pour des objectifs explicites ou implicites, déduit, à partir des données qu'il reçoit, comment générer des résultats tels que des prédictions, du contenu, des recommandations ou des décisions susceptibles d'influencer des environnements physiques ou virtuels. Les différents systèmes d'intelligence artificielle varient dans leurs niveaux d'autonomie et d'adaptabilité après déploiement⁹.

8. Cette définition reflète une compréhension large de ce que sont les systèmes d'intelligence artificielle (systèmes IA), notamment par opposition à d'autres types de systèmes logiciels traditionnels plus simples, fondés sur des règles définies uniquement par des personnes physiques pour exécuter automatiquement des opérations¹⁰. Elle a été rédigée aux fins de la Convention-cadre, sur la base de la définition de l'OCDE de 2023¹¹, et vise à garantir la précision et la sécurité juridiques,

⁷ Convention-cadre, Exposé des motifs accompagnant la définition actualisée d'un système d'intelligence artificielle dans la Recommandation de l'OCDE sur l'intelligence artificielle (OECD/LEGAL/0449, 2019, amendée 2023 [la définition elle-même a été modifiée en 2023, mais la recommandation a fait l'objet de nouvelles modifications en 2024] (*en anglais uniquement*) ; Lignes directrices de la Commission européenne sur la définition d'un système d'intelligence artificielle établie par le règlement (UE) 2024/1689 (loi sur l'IA), *en anglais uniquement* ; Glossaire Cyberjustice de la CEPEJ, ISO/IEC 22989:2022 - Technologies de l'information - Intelligence artificielle - Concepts et terminologie de l'intelligence artificielle (*en anglais uniquement*).

⁸ Les définitions correspondent au glossaire de la CEPEJ sur la cyberjustice, qui est basé sur une série d'autres sources.

⁹ Convention-cadre, article 2.

¹⁰ Convention-cadre, Rapport explicatif, paragraphe 24.

¹¹ Définition actualisée d'un système d'intelligence artificielle dans la recommandation de l'OCDE sur l'intelligence artificielle (OCDE/LEGAL/0449, 2019, modifiée en 2023). Un aperçu simplifié d'un système d'IA figure dans le mémorandum explicatif de

tout en restant suffisamment abstraite et flexible pour rester valable malgré les évolutions technologiques futures. Toutefois, elle n'a pas pour but de donner une signification universelle au terme concerné¹².

2.1.1 Cycle de vie des systèmes d'IA

9. Le cycle de vie d'un système d'intelligence artificielle peut englober toute une série d'activités, en fonction du type de technologie et d'autres éléments contextuels, et évoluer dans le temps. Voici quelques exemples pertinents et non exhaustifs d'activités : (1) planification et conception, (2) collecte et traitement de données, (3) développement de systèmes d'intelligence artificielle, y compris l'élaboration de modèles et/ou l'adaptation de modèles existants à des tâches spécifiques, (4) essais, vérification et validation, (5) fourniture/mise à disposition des systèmes, (6) déploiement, (7) exploitation et surveillance, et (8) mise hors service¹³. Ces activités se déroulent souvent de manière itérative et ne sont pas nécessairement séquentielles. Elles peuvent également recommencer à zéro en cas de modifications substantielles du système ou de son utilisation prévue. La décision de mettre hors service un système d'IA peut intervenir à n'importe quel moment de la phase d'exploitation et de contrôle¹⁴.

2.1.2 Un système basé sur des machines

10. Le terme « basé sur des machines » fait référence au fait que les systèmes d'IA sont développés avec des machines et fonctionnent sur celles-ci. Le terme « machine » peut être compris comme incluant à la fois les composants matériels et logiciels qui permettent au système d'IA de fonctionner. Les composants matériels désignent les éléments physiques de la machine, tels que les unités de traitement, la mémoire, les dispositifs de stockage, les unités de mise en réseau et les interfaces d'entrée/sortie, qui fournissent l'infrastructure nécessaire au calcul. Les composants logiciels englobent le code informatique, les instructions, les programmes, les systèmes d'exploitation et les applications qui gèrent la manière dont le matériel traite les données et exécute les tâches¹⁵.

l'OCDE, p. 7, en anglais uniquement. Cette définition est également utilisée dans la loi européenne sur l'IA, article 3, paragraphe 1.

¹² Rapport explicatif, paragraphe 24. Bien que cette définition permette aux parties à la Convention-cadre de s'entendre sur ce que sont les systèmes d'intelligence artificielle, les parties peuvent la préciser davantage dans leurs systèmes juridiques nationaux afin de renforcer la sécurité juridique et la précision, sans en limiter la portée.

¹³ Rapport explicatif de la Convention-cadre, paragraphe 15.

¹⁴ Idem.

¹⁵ Lignes directrices de la Commission européenne sur la définition d'un système d'intelligence artificielle établi par la loi sur l'IA, paragraphe 11 (*en anglais uniquement*)

2.1.3 L'autonomie

11. L'autonomie d'un système d'IA désigne le degré auquel un système peut apprendre ou agir sans intervention humaine après la délégation de l'autonomie et l'automatisation des processus par les humains. La supervision humaine peut avoir lieu à n'importe quelle étape du cycle de vie du système d'IA¹⁶. Certains systèmes d'IA peuvent générer des résultats sans que ceux-ci soient explicitement décrits dans l'objectif du système d'IA et sans instructions spécifiques de la part d'un humain¹⁷.

2.1.4 La capacité d'adaptation

12. La capacité d'adaptation désigne la capacité d'un système d'IA à évoluer et à modifier son comportement par une interaction directe avec les entrées et les données avant ou après son déploiement. Il s'agit par exemple d'un système de reconnaissance vocale qui s'adapte à la voix d'un individu ou d'un système de recommandation musicale personnalisé. Les systèmes d'IA peuvent être formés une seule fois, de manière périodique ou en continu, et fonctionnent en inférant des schémas et des relations à partir des données. Grâce à cet entraînement, certains systèmes d'IA peuvent développer la capacité d'effectuer de nouvelles formes d'inférence qui n'avaient pas été initialement envisagées par leurs concepteurs¹⁸.

2.1.5 Les objectifs du système d'IA

13. Les systèmes d'IA sont conçus pour fonctionner selon un ou plusieurs objectifs. Les objectifs du système peuvent être définis de manière explicite ou implicite. Les objectifs explicites se réfèrent à des buts clairement énoncés qui sont directement encodés par le développeur dans le système. Ils peuvent, par exemple, être formulés comme l'optimisation d'une fonction de coût, d'une probabilité ou d'une récompense cumulée. Les objectifs implicites renvoient à des buts qui ne sont pas explicitement énoncés, mais qui peuvent être déduits du comportement ou des hypothèses sous-jacentes du système. Ces objectifs peuvent découler des données d'entraînement ou de l'interaction du système d'IA avec son environnement¹⁹.

¹⁶ En anglais uniquement ; traduction libre. Exposé des motifs de l'OCDE, p. 6.

¹⁷ Idem.

¹⁸ Idem.

¹⁹ Lignes directrices de la Commission européenne sur la définition d'un système d'intelligence artificielle établi par la loi sur l'IA, paragraphe 4 (en anglais uniquement). Voir également l'exposé des motifs de l'OCDE, p. 7.

2.1.6 L'environnement ou le contexte

14. Un environnement ou un contexte en relation avec un système d'IA est un espace observable ou partiellement observable, perçu à l'aide de données et d'entrées de capteurs et influencé par des actions (par l'intermédiaire d'actionneurs). Les environnements influencés par les systèmes d'IA peuvent être physiques ou virtuels et inclure des environnements décrivant des aspects de l'activité humaine, tels que les signaux biologiques ou le comportement humain. Les capteurs et les actionneurs sont soit des êtres humains, soit des composants de machines ou d'appareils²⁰.

2.1.7 Les données d'entrée

15. Les données d'entrée sont utilisées à la fois pendant le développement et après le déploiement. Les données d'entrée peuvent prendre la forme de connaissances, de règles et de codes que les humains introduisent dans le système au cours du développement ou de données. Les humains et les machines peuvent fournir des données. Au cours du développement, les données sont exploitées pour construire des systèmes d'IA, par exemple avec l'apprentissage automatique qui produit un modèle à partir de données d'apprentissage et/ou de données humaines. Les données sont également utilisées par un système en fonctionnement, par exemple pour déduire comment générer des résultats. Les données d'entrée peuvent inclure des données pertinentes pour la tâche à effectuer ou prendre la forme, par exemple, d'une invite de l'utilisateur ou d'une requête de recherche²¹.

2.1.8 L'inférence

16. Le concept d'« inférence » fait généralement référence à l'étape au cours de laquelle un système génère des données de sortie à partir de ses données d'entrées, généralement après le déploiement. L'expression « déduire comment générer des données de sorties » doit être comprise comme faisant également référence à la phase de construction du système d'IA, au cours de laquelle un modèle est dérivé des entrées/données²².

²⁰ Idem, p. 7.

²¹ Idem, p. 8.

²² Idem, p. 9 ; voir aussi les Lignes directrices de la Commission européenne, paragraphe 26 et suivants.

2.1.9 Les données de sortie

17. Les données de sortie reflètent généralement les différentes tâches ou fonctions exécutées par les systèmes d'IA. Elles peuvent être classées en grandes catégories : recommandations, prédictions, contenu et décisions. Ces catégories correspondent à différents niveaux d'implication humaine, les « décisions » étant le type de donnée le plus autonome (le système d'IA influence directement son environnement ou demande à une autre entité de le faire) et les « prédictions » le moins autonome. Elles comprennent, sans s'y limiter, la reconnaissance (identification et catégorisation des données, par exemple : image, vidéo, audio et texte, en classifications spécifiques, ainsi que la segmentation d'images et la détection d'objets), la détection d'événements (relier des points de données pour détecter des modèles, ainsi que des cas particuliers ou des anomalies), la prévision (utiliser les comportements passés et existants pour prédire les résultats futurs), la personnalisation (développer le profil d'un individu et apprendre et adapter ses résultats à cet individu au fil du temps), l'aide à l'interaction l'interprétation et la création de contenu pour alimenter les conversations et autres interactions entre les machines et les humains, pouvant impliquer plusieurs médias tels que la voix, le texte et les images), la génération de contenu (y compris, mais sans s'y limiter, l'optimisation axée sur les objectifs : trouver la solution optimale à un problème pour une fonction de coût ou un objectif prédéfini) et le raisonnement avec des structures de connaissances (déduire de nouveaux résultats possibles même s'ils ne sont pas présents dans les données existantes, grâce à la modélisation et à la simulation)²³.

2.2 Autres concepts techniques pertinents pour l'IA et les droits humains

2.2.1 La transparence

18. Dans le contexte de l'IA, la transparence fait référence à l'ouverture et à la clarté dans la gouvernance des activités au cours du cycle de vie des systèmes d'IA. Cela signifie que les processus décisionnels et le fonctionnement général des systèmes d'IA doivent être compréhensibles et accessibles aux acteurs appropriés de l'IA et, le cas échéant, aux parties prenantes concernées²⁴. Les moyens d'assurer la transparence dépendraient de nombreux facteurs différents, tels que, par exemple, le type de système d'intelligence artificielle, le contexte de son

²³ Voir l'Exposé des motifs de l'OCDE, p. 9 ; voir également les lignes directrices de la Commission européenne, paragraphe 52 et suivants.

²⁴ Voir le rapport explicatif de la Convention-cadre, paragraphe 57. Voir également le principe de l'OCDE sur la transparence et l'explicabilité (Recommandation du Conseil de l'OCDE sur l'intelligence artificielle, OCDE/LEGAL/0449 et ISO/IEC 22989 : 2022, 5.15.8).

utilisation ou son rôle, et le contexte de l'acteur concerné ou de la partie prenante affectée. En outre, les mesures pertinentes comprennent, le cas échéant, l'enregistrement d'éléments clés tels que la provenance des données, les méthodologies d'entraînement, la validité des sources de données, la documentation et la transparence sur les données d'entraînement, de test et de validation utilisées, les efforts d'atténuation des risques, ainsi que les processus et les décisions mis en œuvre, afin de faciliter une compréhension globale de la manière dont les résultats du système d'intelligence artificielle sont obtenus et ont un impact sur les droits humains, la démocratie et l'État de droit.²⁵

19. À cette fin, l'utilisation de logiciels libres et de normes techniques interopérables devrait être encouragée pour les systèmes d'IA, dans la mesure où cela contribue à la transparence et à la vérifiabilité des systèmes, ainsi qu'à la contestabilité des résultats.²⁶ Les systèmes d'IA utilisés dans des contextes susceptibles d'avoir une incidence sur les droits humains, tels que les processus électoraux, devraient conserver des journaux d'audit complets et inviolables, permettant de retracer toutes les décisions et actions effectuées.²⁷ Ces journaux devraient être conservés conformément aux délais légaux applicables et rester accessibles aux autorités de contrôle compétentes, sous réserve de garanties appropriées en matière de protection des données.²⁸

2.2.2 L'explicabilité

20. L'explicabilité est une composante particulièrement importante de la transparence. Les systèmes d'IA intégrant l'apprentissage automatique (« Machine Learning » ou « ML ») s'appuient sur des modèles mathématiques dérivés du traitement automatique des données, plutôt que sur une programmation explicite par des humains. Il est donc difficile, même pour les experts en IA, y compris les développeurs de systèmes, de comprendre comment leurs résultats sont ensuite produits²⁹. L'opacité

²⁵ Voir le rapport explicatif de la Convention-cadre, paragraphe 57.

²⁶ Recommandation du Conseil de l'OCDE sur l'intelligence artificielle (Principes de l'OCDE en matière d'IA) et rapport de l'OCDE, *Advancing Accountability in AI Governing and Managing Risks Throughout The Lifecycle For Trustworthy AI* (2023), en anglais uniquement.

²⁷ Rapport de l'OCDE, *Advancing Accountability in AI Governing and Managing Risks Throughout The Lifecycle For Trustworthy AI* (2023), en anglais uniquement ; voir également la *Déclaration interprétative du code de bonne conduite en matière électorale sur les technologies numériques et l'intelligence artificielle* (CDL-AD(2024)044), Commission européenne pour la démocratie par le droit (Commission de Venise), paragraphes 36-39.

²⁸ Voir la recommandation de l'UNESCO sur l'éthique de l'intelligence artificielle, paragraphe 51.

²⁹ TechDispatch : Explainable Artificial Intelligence, European Data Protection Supervisor (2023), citant Peters, U (*en anglais uniquement*). 'Explainable AI lacks

ou l'effet « boîte noire » qui en résulte rend non seulement les décisions plus difficiles à comprendre, mais elle peut également avoir un impact direct sur les individus puisqu'elle peut masquer les lacunes dans les systèmes d'IA, telles que l'existence de biais, d'inexactitudes ou de ce que l'on appelle des « hallucinations ».

21. L'« explicabilité » désigne donc la capacité à fournir, sous réserve de faisabilité technique et compte tenu de l'état de la technique généralement reconnu, des explications suffisamment compréhensibles sur les raisons pour lesquelles un système d'intelligence artificielle fournit des informations, produit des prédictions, des contenus, des recommandations ou des décisions, ainsi qu'une compréhension générale de ses capacités et de ses limites³⁰. Il s'agit de l'idée que le résultat d'un système ou d'un algorithme automatisé peut être expliqué d'une manière qui « ait du sens » pour les personnes, permettant à celles qui ont été affectées par un résultat de le comprendre et de le contester. Cela comprend la fourniture, en termes clairs et simples, et de manière appropriée au contexte, des principaux facteurs pris en compte dans une décision, des facteurs déterminants et des données, de la logique ou de l'algorithme utilisés pour parvenir à une décision.³¹

2.2.3 L'interprétabilité

22. L'interprétabilité désigne la capacité à comprendre comment un système d'intelligence artificielle établit ses prédictions ou prend ses décisions ou, en d'autres termes, la mesure dans laquelle les résultats des systèmes d'intelligence artificielle peuvent être rendus accessibles et compréhensibles tant pour les experts que pour les non-experts. Elle implique de rendre le fonctionnement interne, la logique et les processus décisionnels des systèmes d'intelligence artificielle compréhensibles et accessibles aux utilisateurs humains, y compris les développeurs, les parties prenantes et les utilisateurs finaux, ainsi qu'aux personnes concernées³².

regulative reasons : why AI and human decision-making are not equally opaque', (AI and Ethics 2023) ; voir également : CDDH-IA(2024)09, Résumé de l'échange de vues avec des expert.e.s indépendant.e.s externes et des représentant.e.s des comités intergouvernementaux du Conseil de l'Europe (25 septembre), points clés soulevés par Marko Grobelnik et CDDH-IA(2024)07, Compilation des contributions écrites et des présentations reçues des experts de l'échange de vues de la 1^{re} réunion, pp. 3-16.

³⁰ Rapport explicatif de la Convention-cadre, paragraphe 60. Voir aussi ISO/IEC 22989:2022, 5.15.6.

³¹ OCDE, *AI and the future of social protection in OECD countries*, OECD Artificial Intelligence Papers, 2025, n° 42, p. 20, en anglais uniquement.

³² Rapport explicatif, paragraphe 61.

3. DROITS HUMAINS ET INTELLIGENCE ARTIFICIELLE

3.1 Questions générales

23. Cette section donne un aperçu de la CEDH, de la CSE et de la Convention-cadre en soulignant les principes généraux de la CEDH et de la CSE qui peuvent régir la protection des droits dans le contexte de l'IA. Elle met également en évidence les principes pertinents de la Convention-cadre lorsqu'ils offrent des orientations précieuses dans le cadre de la CEDH et de la CSE. En outre, elle examine les défis récurrents en matière de droits humains qui peuvent se poser en relation avec l'utilisation des systèmes d'IA.

3.1.1 La Convention européenne des droits de l'homme (CEDH)

24. La CEDH est le principal instrument du Conseil de l'Europe en matière de droits humains. Elle fixe des normes contraignantes pour les autorités publiques des États membres. La Cour européenne des droits de l'homme veille au respect de la mise en œuvre de la CEDH par les États. Les particuliers, les groupes, les personnes morales et les organisations non gouvernementales (ONG) peuvent porter plainte devant la Cour pour des violations présumées des droits humains, une fois que toutes les voies de recours internes ont été épuisées.

3.1.2 La Charte sociale européenne (CSE)

25. En tant qu'instrument central des droits économiques et sociaux au sein du Conseil de l'Europe, la CSE garantit des protections fondamentales qui complètent la CEDH. La Charte sociale européenne révisée (CSE (Révisée)) intègre de nouveaux droits et amendements. 42 des 46 États membres du Conseil de l'Europe sont parties à la CSE ou à la CSE (Révisée)³³. Le Comité européen des droits sociaux (CEDS) assure le suivi de la Charte par le biais de deux mécanismes : (i) les rapports réguliers des États parties sur leur mise en œuvre de la CSE et (ii) les réclamations collectives déposées par les partenaires sociaux et les organisations non gouvernementales (ONG), pour les États ayant ratifié le Protocole additionnel de 1995 à la Charte sociale européenne prévoyant un système de réclamations collectives³⁴. Dans la mesure où elles se réfèrent à des dispositions juridiques contraignantes et sont adoptées par un organe de contrôle établi par la CES, les conclusions et décisions du CEDS constituent une interprétation faisant autorité, bien que

³³ Le Liechtenstein, Monaco, Saint-Marin et la Suisse ne sont parties à aucun de ces traités.

³⁴ 16 des 42 parties à la CSE ont ratifié ce protocole additionnel.

non contraignante sur le plan juridique, des dispositions de la CSE. Bien que ses décisions et conclusions ne soient pas directement exécutoires, elles représentent une interprétation faisant autorité des dispositions de la CSE. Les États parties ont l'obligation de coopérer avec le CEDS et de prendre en compte ses décisions et conclusions qui découlent de l'application du principe de bonne foi au respect de leurs obligations conventionnelles en vertu de la CSE.

3.1.3 La Convention-cadre sur l'intelligence artificielle et les droits de l'homme, la démocratie et l'État de droit

26. La **Convention-cadre** renforce les normes internationales existantes (telles que la CEDH et la CSE) qui peuvent être applicables à chaque Partie.³⁵ Elle adopte une approche neutre sur le plan technologique, en se concentrant sur les principes plutôt qu'en réglementant des technologies spécifiques. Elle s'applique aux activités menées par les autorités publiques (y compris les acteurs privés agissant en leur nom)³⁶. En ce qui concerne les activités menées par des acteurs privés agissant de manière indépendante, les États parties s'engagent à traiter les risques et les impacts d'une manière conforme à l'objet et au but de la Convention-cadre, soit en appliquant directement les principes et obligations énoncés dans la Convention, soit en prenant « d'autres mesures appropriées »³⁷. En outre, les questions relatives à la défense nationale n'entrent pas dans le champ d'application du traité³⁸, ainsi que : (i) les activités liées à la protection des « intérêts de sécurité nationale » des États parties, étant entendu que ces activités sont menées d'une manière conforme au droit international applicable, y compris aux obligations internationales en matière de droits humains, et dans le respect des institutions et processus démocratiques de chaque partie³⁹ ; (ii) les activités de recherche et de développement, à moins que les essais ou activités similaires ne soient entrepris d'une manière susceptible de porter atteinte aux droits humains, à la démocratie et à l'État de droit⁴⁰.

³⁵ Dans l'UE, la Convention-cadre doit être mise en œuvre exclusivement par le biais du règlement (UE) 2024/1689 du Parlement européen et du Conseil (loi sur l'IA) et d'autres acquis pertinents de l'Union, le cas échéant.

³⁶ Convention-cadre, Article 3, paragraphe 1 (a).

³⁷ Article 3, paragraphe 1 (b).

³⁸ Article 3, paragraphe 4. Notez également qu'en vertu de l'article 1.d. de son statut, « les questions relatives à la défense nationale ne relèvent pas du Conseil de l'Europe ».

³⁹ Article 3, paragraphe 2.

⁴⁰ Article 3, paragraphe 3.

27. Les activités du cycle de vie des systèmes d'IA doivent respecter les principes suivants⁴¹ :

- Dignité humaine et autonomie personnelle
- Transparence et contrôle
- Obligation de rendre des comptes et responsabilité
- Égalité et non-discrimination
- Respect de la vie privée et protection des données à caractère personnel
- Fiabilité
- Innovation sûre

28. Les principales exigences comprennent la disponibilité de recours, dans la mesure où ceux-ci sont requis par les obligations internationales d'une Partie en cas de violations des droits humains liées à l'IA, ⁴² la garantie de garanties procédurales pour les personnes concernées, y compris en veillant à ce que, selon le contexte, les personnes interagissant avec des systèmes d'IA soient informées⁴³ ; la réalisation d'évaluations des risques et des incidences sur les droits humains, la démocratie et l'État de droit⁴⁴ ; et la possibilité d'interdire, de suspendre ou de prendre d'autres mesures appropriées à l'égard de certaines utilisations des systèmes d'IA que l'État partie considère comme incompatibles avec le respect des droits humains, le fonctionnement de la démocratie ou l'état de droit.⁴⁵ La Convention-cadre prévoit également des mécanismes de suivi et de coopération et introduit un mécanisme de contrôle obligatoire.⁴⁶

29. Compte tenu de la complexité technique du sujet, le HUDERIA (Évaluation des risques et des impacts des systèmes d'intelligence artificielle (IA) du point de vue des droits humains, de la démocratie et de l'État de droit)⁴⁷ du Conseil de l'Europe fournit des orientations

⁴¹ Chapitre III (articles 6 à 13)

⁴² Chapitre IV (article 14)

⁴³ Article 15 : « Lorsqu'un système d'intelligence artificielle contribue en grande partie à la prise des décisions ou prend des décisions ayant un impact sur les droits de l'homme, des garanties procédurales effectives devraient, par exemple, inclure un contrôle humain, y compris un examen ex ante ou ex post de la décision par des êtres humains. » (Rapport explicatif, paragraphe 103).

⁴⁴ Chapitre V (article 16).

⁴⁵ Article 16, paragraphe 4.

⁴⁶ Chapitre VII (articles 23 à 26).

⁴⁷ Le HUDERIA est un guide autonome, non contraignant juridiquement, qui n'a pas d'effet juridique. Il n'est pas obligatoire et n'est pas destiné à servir d'aide à l'interprétation de la Convention-cadre. En outre, bien que le HUDERIA ait un rôle facilitateur, il ne constitue pas un moyen de mettre en œuvre la Convention-cadre. De nombreux cadres, politiques, guides, normes ou outils existants ou futurs peuvent être utilisés pour aider à la gestion des risques et des impacts de l'IA, y compris le

supplémentaires non contraignantes sur la manière de mettre en œuvre et d'appliquer les obligations de la Convention-cadre en matière d'évaluation des risques et des impacts des systèmes d'IA.⁴⁸ Il se situe à l'intersection des normes internationales en matière de droits humains et des cadres techniques existants sur la gestion des risques dans le contexte de l'IA, en encourageant le développement d'une IA sûre, sécurisée et fiable, à la fois performante et favorisant le respect des droits humains, de la démocratie et de l'État de droit. Ce manuel peut fournir des informations complémentaires utiles à ceux qui appliquent HUDERIA.

3.1.4 Les principes généraux de la CEDH et de la CSE dans le contexte de l'IA

30. Il n'existe à ce jour que des orientations limitées de la Cour et du CEDS concernant l'impact des technologies d'IA sur les droits garantis par la CEDH et la CSE.⁴⁹ Cependant, les principes établis dans le cadre de la CEDH et de la CSE fournissent des indications sur la manière dont ces traités peuvent s'appliquer aux défis liés à l'IA en matière de droits humains. Si certains principes sont communs aux deux traités, d'autres sont spécifiques à l'un ou à l'autre.⁵⁰

Protection effective des droits

31. La CEDH et la CSE visent à garantir des droits qui ne sont pas simplement théoriques ou illusoires, mais pratiques et effectifs⁵¹. Les autorités nationales doivent veiller à ce que les détenteurs de droits

HUDERIA. Les parties à la Convention-cadre ont la possibilité d'utiliser ou d'adapter le guide, en tout ou en partie, pour élaborer de nouvelles approches en matière d'évaluation des risques ou d'utiliser ou d'adapter les approches existantes conformément à leurs lois applicables, à condition que les parties respectent pleinement leurs obligations au titre de la Convention-cadre, y compris les critères de référence pour la gestion des risques et des impacts énoncés dans son chapitre V.

⁴⁸ Convention-cadre, article 16.

⁴⁹ Bien que la Cour n'ait pas encore abordé directement l'IA, elle a examiné des affaires impliquant de nouvelles technologies et leur impact sur les droits humains, y compris les technologies intégrant des fonctionnalités d'IA, telles que les systèmes de reconnaissance faciale. (voir *Glukhin c. Russie*, Requête n° 11519/20, 4 juillet 2023. Voir également Factsheet – New technologies (*en anglais uniquement*)).

⁵⁰ Les systèmes conventionnels de la CEDH et de la CSE sont complémentaires et interdépendants. La Cour a précisé qu'il n'y a pas de division étanche entre les droits civils et politiques et les droits économiques, sociaux et culturels. Voir *Airey c. Irlande*, 9 octobre 1979, 6289/73, paragraphe 24 ; voir aussi Digest of Case Law of the European Committee of Social Rights, décembre 2022, p. 33, en anglais uniquement.

⁵¹ *Airey c. Irlande*, n° 6289/73, 9 octobre 1979, paragraphe 24 ; *Commission internationale de juristes (CIJ) c. Portugal*, réclamation n° 1/1998, décision sur le bien-fondé du 9 septembre 1999, paragraphe 32 ; *Fédération européenne des associations nationales travaillant avec les sans-abris (FEANTSA) c. Slovaquie*, réclamation n° 53/2008, décision sur le bien-fondé du 8 septembre 2009, paragraphe 28.

puissent effectivement jouir de leurs droits, ce qui implique non seulement d'adopter une législation, mais aussi de veiller à son application effective, de fournir des ressources adéquates et d'établir des procédures opérationnelles appropriées. En conséquence, les États devraient garantir la protection effective des droits humains contre les atteintes liées aux activités relevant du cycle de vie des systèmes d'IA, grâce à des mesures pouvant inclure l'adoption ou la mise en œuvre de lois, la fourniture de ressources, la création ou la désignation de structures nationales de défense des droits humains existantes, telles que les institutions nationales des droits humains (INDH), en tant que mécanismes de contrôle indépendants, et la garantie d'une coopération efficace entre ces mécanismes et d'autres structures nationales de défense des droits humains.

Subsidiarité et la marge d'appréciation

32. La subsidiarité signifie que les États ont la responsabilité première de garantir à toute personne relevant de leur juridiction les droits et libertés définis dans la CEDH.⁵² La Cour interprète la CEDH avec autorité et agit en tant que garant des personnes dont les droits et libertés ne sont pas garantis au niveau national.⁵³

33. Les autorités nationales peuvent bénéficier d'une « marge d'appréciation » dans la manière dont elles appliquent et mettent en œuvre la CEDH, en fonction des circonstances de l'affaire et des droits et libertés en jeu. Cela reflète le fait que le système de la CEDH est subsidiaire par rapport à la sauvegarde des droits humains au niveau national et que les autorités nationales sont en principe mieux placées qu'une cour internationale pour évaluer les besoins et les conditions locales⁵⁴. En vertu de la Charte, les États parties disposent également d'un pouvoir discrétionnaire pour déterminer les mesures à prendre pour se conformer à ses dispositions, en mettant en balance les intérêts généraux avec les besoins de groupes spécifiques et les ressources disponibles. En ce qui concerne les nouvelles technologies, en particulier, tout État qui revendique un rôle de pionnier dans leur développement a la responsabilité particulière de trouver le juste équilibre entre les avantages potentiels de leur utilisation à grande échelle et les droits protégés⁵⁵.

⁵² CEDH, préambule, considérant 7.

⁵³ Rapport explicatif, Protocole n° 15 portant amendement à la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales (STCE n° 213), paragraphe 8

⁵⁴ Idem, paragraphe 9

⁵⁵ *S. et Marper c. Royaume-Uni* [GC], n° 30562/04 et n° 30566/04, 4 décembre 2008, paragraphe 112 : « La Cour considère que tout État qui revendique un rôle de pionnier dans l'évolution de nouvelles technologies porte la responsabilité particulière de trouver le juste équilibre en la matière. »

Interprétation évolutive et doctrine de 'l'instrument vivant'

34. La CEDH et la CSE sont des « instruments vivants », interprétés de manière dynamique à la lumière des conditions actuelles pour répondre aux enjeux sociétaux et technologiques en constante évolution⁵⁶. Les arrêts antérieurs de la Cour sur des sujets tels que l'interception des données⁵⁷, les données biométriques⁵⁸, internet et les outils numériques⁵⁹ ou la technologie de reconnaissance faciale⁶⁰ soulignent sa capacité à adapter l'application des droits existants aux défis modernes. De même, le CEDS a abordé le droit à la vie privée dans le contexte des nouvelles technologies émergentes⁶¹. En appliquant cette doctrine, la Cour et le CEDS devraient tous deux appliquer la CEDH et la CSE aux affaires liées à l'IA à l'avenir.

Obligations positives

35. Les États ont le devoir, en vertu de la CEDH et de la CSE, de s'abstenir de toute ingérence injustifiée dans les droits humains (« obligations négatives ») et d'assurer leur réalisation et leur protection effectives (« obligations positives »). Les obligations positives de fond exigent les mesures de base nécessaires à la pleine jouissance des droits garantis (par exemple, des règles appropriées régissant l'intervention de la police ou interdisant les mauvais traitements). Les obligations positives de procédure exigent des procédures nationales pour assurer la protection des détenteurs de droits (par exemple, mener une enquête efficace).

36. Les obligations positives s'appliquent même dans les cas où les menaces proviennent de personnes privées ou d'entités échappant au contrôle direct de l'État, car ces instruments concernent à la fois les relations verticales - entre les autorités nationales et les individus - et les relations horizontales⁶², qui impliquent des interactions entre les individus

⁵⁶ *Tyrer c. Royaume-Uni*, n° 5856/72, 25 avril 1978, paragraphe 31 ; *Transgender-Europe et ILGA-Europe c. République tchèque*, n° 117/2015, 15 mai 2018, paragraphe 75 ; *Défense des enfants international (DEI) c. Pays-Bas*, n° 47/2008, 20 octobre 2009, paragraphe 29.

⁵⁷ *Big Brother Watch et autres c. Royaume-Uni* [GC], n° 58170/13, n° 62322/14 et n° 24960/15, 25 mai 2021.

⁵⁸ *S. et Marper c. Royaume-Uni* [GC], n° 30562/04 et n° 30566/04, 4 décembre 2008.

⁵⁹ *Ahmet Yıldırım c. Turquie*, n° 3111/10, 18 mars 2013 ; *Magyar Helsinki Bizottság c. Hongrie* [GC], n° 18030/11, 8 novembre 2016.

⁶⁰ *Glukhin c. Russie*, n° 11519/20, 4 juillet 2023.

⁶¹ CEDS, Conclusions 2012, Statement of Interpretation on Article 1 paragraphe 2 (*en anglais uniquement*)

⁶² La Cour a reconnu le devoir des États de protéger les droits humains dans ces contextes horizontaux, tels que le droit au respect de la vie privée et familiale (article 8 de la CEDH), voir *X et Y c. Pays-Bas*, n° 8978/80, 26 mars 1985, paragraphe 23 ; la liberté d'expression (article 10 de la CEDH), voir *Plate-forme « Ärzte für das Leben »*

ou les entités. Les États peuvent être tenus de protéger les droits humains dans la sphère des relations entre les individus eux-mêmes (effet horizontal). Cette obligation revêt une importance particulière dans le contexte du déploiement des systèmes d'IA, où les partenariats public-privé et les achats auprès d'acteurs privés sont prédominants.

37. Les États doivent agir avec diligence et de manière raisonnable, en prenant les mesures appropriées dans la limite de leurs ressources et de leurs capacités. Les obligations positives peuvent exiger de l'État qu'il veille à l'existence de mécanismes adéquats et efficaces permettant d'imposer des sanctions dans des cas particuliers, qu'il adopte des règles juridiques spécifiques et/ou qu'il prenne des mesures opérationnelles pour protéger les individus contre les risques prévisibles pesant sur leurs droits.⁶³

38. Les obligations positives des États⁶⁴ peuvent donc les contraindre à prendre les mesures nécessaires pour protéger les droits humains, y compris, si nécessaire, à évaluer les risques et les impacts potentiels sur les droits humains que peuvent présenter les systèmes d'IA et à envisager des mesures pour remédier efficacement à ces préjudices potentiels et/ou à mettre en œuvre des mesures pour atténuer les risques. La Convention-cadre contient une disposition spécifique prescrivant la nécessité d'identifier, d'évaluer, de prévenir et d'atténuer *ex ante* et, le cas échéant, de manière itérative tout au long du cycle de vie du système d'IA, les risques pertinents et les impacts potentiels sur les droits humains, la démocratie et l'État de droit en suivant et en permettant le développement d'une méthodologie avec des critères concrets et objectifs pour de telles évaluations⁶⁵.

c. *Autriche*, n° 10126/82, 21 juin 1986, paragraphe 23 ; et la liberté d'association (article 11 de la CEDH), voir *Khurshid Mustafa et Tarzibachi c. Suède*, n° 23883/06, 16 décembre 2008, paragraphe 32 ; *Parti populaire chrétien-démocrate c. Moldova* (n° 2), n° 25196/04, 2 février 2010, paragraphe 25.

⁶³ Pour la CEDH, voir par exemple, *Osman c. Royaume-Uni* [GC], nos 87/1997/871/1083, paragraphe 115. Pour la CSE, voir, par exemple, CEDS, Conclusions 2020, Albanie sur l'article 1 paragraphe 2, Conclusions 2005, Déclaration interprétative sur l'article 11, *Fédération internationale pour la planification familiale - Réseau européen (IPPF EN) c. Italie*, réclamation n° 87/2012, décision sur le fond du 10 septembre 2013, paragraphe 66 ; voir également *Confédération générale italienne du travail (CGIL) c. Italie*, n° 91/2013, 12 octobre 2015, paragraphes 162 et 190.

⁶⁴ Voir ci-dessous, section 3.2.1.

⁶⁵ Article 16 de la Convention-cadre, voir également le Rapport explicatif, paragraphe 105.

Dignité humaine

39. Dans le système de la CEDH, la dignité humaine est invoquée par la Cour pour affirmer la valeur intrinsèque et l'égalité des individus⁶⁶. La Cour a déclaré que « le respect de la dignité humaine fait partie de l'essence même de la Convention »⁶⁷. Le système de la CSE reconnaît également que la dignité humaine est la valeur fondamentale et le cœur même du droit européen positif en matière de droits humains, que ce soit dans le cadre de la Charte sociale européenne ou de la Convention européenne des droits de l'homme.⁶⁸

40. La Convention-cadre exige également que le respect de la dignité humaine figure parmi les principes qui régissent l'intelligence artificielle.⁶⁹ Les activités du cycle de vie de l'IA ne doivent pas déshumaniser les individus, porter atteinte à leur autonomie ou les réduire à des points de données, et l'IA ne doit pas être anthropomorphisée d'une manière qui porte atteinte à la dignité humaine⁷⁰.

Autonomie personnelle et autodétermination

41. L'autonomie personnelle est un principe important qui sous-tend l'interprétation des garanties de la CEDH⁷¹. Elle constitue un aspect important de la dignité humaine et renvoie à la capacité d'autodétermination des individus, c'est-à-dire à leur aptitude à faire des choix et à prendre des décisions, y compris sans contrainte, et à vivre leur vie librement. Dans le contexte de l'IA, l'autonomie individuelle exige que les individus aient le contrôle de l'utilisation et de l'impact des technologies de l'IA dans leur vie, et que leur agence et leur autonomie ne soient pas diminuées pour autant⁷². La Convention-cadre exige également expressément que le respect de l'autonomie individuelle figure parmi les principes qui régissent l'intelligence artificielle⁷³.

⁶⁶ *Lăcătuș c. Suisse*, requête, n° 14065/15, Arrêt (au principal et satisfaction équitable), 19 janvier 2021.

⁶⁷ *Magyar Helsinki Bizottság c. Hongrie* [GC], n° 18030/11, Arrêt (au principal et satisfaction équitable), 8 novembre 2016, paragraphe 155.

⁶⁸ *Fédération internationale pour les droits humains (FIDH) c. France*, n° 14/2003, 8 septembre 2004, paragraphe 31.

⁶⁹ Convention-cadre, article 7.

⁷⁰ Rapport explicatif, paragraphe 53.

⁷¹ *Pretty c. Royaume-Uni*, n° 2346/02, paragraphe 61 et arrêt [GC] du 11 janvier 2006, *Sorensen et Rasmussen c. Danemark*, n° 52562/99 et 52620/99, paragraphe 54. Voir également le préambule de la Convention 108 sur la protection des données, telle qu'elle sera modifiée à la suite de l'entrée en vigueur du protocole modificatif.

⁷² Rapport explicatif de la Convention-cadre, paragraphe 55.

⁷³ Convention-cadre, article 7.

Légalité, but légitime, nécessité, proportionnalité et juste équilibre

42. Certains droits de la CEDH sont absolus et ne peuvent faire l'objet de dérogations en cas d'urgence, d'exception ou d'ingérence autorisée. Toutefois, les États parties sont autorisés à restreindre certains droits énoncés dans la CEDH⁷⁴ et la CSE⁷⁵, appelés « droits relatifs », qui permettent d'assurer un équilibre entre les intérêts individuels et les intérêts généraux. La CEDH et la CSE prévoient certaines exigences générales qui doivent être satisfaites pour qu'une ingérence soit justifiée. L'ingérence doit être (i) 'prévues par la loi' ou 'conforme à la loi' (condition de légalité)⁷⁶. Cela signifie qu'elle doit avoir une base claire dans le droit national, garantissant qu'elle est ancrée dans des cadres juridiques établis. En outre, la base juridique doit être accessible au public, ce qui signifie que les individus peuvent connaître et comprendre les lois qui affectent leurs droits.⁷⁷ L'ingérence doit également être prévisible, ce qui permet aux personnes d'anticiper comment et quand leurs droits pourraient être restreints⁷⁸. Enfin, elle doit être exempte d'arbitraire et mise en œuvre avec des garanties procédurales appropriées pour assurer l'équité et la diligence⁷⁹. L'ingérence dans le droit doit (ii) poursuivre un but légitime⁸⁰ et elle doit être (iii) nécessaire (dans une société démocratique)

⁷⁴ Aucune dérogation n'est autorisée en temps de guerre à certaines dispositions de la CEDH et de ses protocoles : le droit à la vie en vertu de l'article 2 (sauf en cas de décès résultant d'actes de guerre licites) ; l'interdiction de la torture et des peines ou traitements inhumains ou dégradants en vertu de l'article 3 ; l'interdiction de l'esclavage et de la servitude en vertu de l'article 4 (mais pas l'interdiction du travail forcé ou obligatoire en vertu de l'article 4(2)) ; l'interdiction des peines non prévues par la loi en vertu de l'article 7 ; l'abolition de la peine de mort en temps de paix (Protocole n° 6, article 1) ; le droit de ne pas être jugé ou puni deux fois (ne bis in idem) (Protocole n° 7, article 4) ; et l'abolition de la peine de mort en toutes circonstances (Protocole n° 13, article 1). La Convention prévoit des exceptions à certains droits, comme le droit de ne pas être arbitrairement privé de liberté en vertu de l'article 5. Dans de tels cas, la Cour a clairement établi que la liste des exceptions dans un article donné est exhaustive et que seule une interprétation étroite de ces exceptions est conforme à l'objectif de cet article.

⁷⁵ Les États parties sont autorisés à restreindre les droits inscrits dans la Charte sociale européenne. Ces conditions de restriction sont énoncées à l'article 31 de la CSE et l'article G de la Charte sociale européenne révisée.

⁷⁶ *Leyla Şahin c. Turquie* [GC], Requête n° 44774/98, 10 novembre 2005, paragraphe 88 (avec de nombreuses autres références) ; *Biržietis c. Lituanie*, Requête n° 49304/09, 14 juin 2016, paragraphe 50.

⁷⁷ *The Sunday Times c. Royaume-Uni* (n° 1), requête n° 6538/74, 26 avril 1979, paragraphe 48.

⁷⁸ Idem.

⁷⁹ *R.Sz. c. Hongrie*, requête n° 41838/11, 2 juillet 2013, paragraphe 36.

⁸⁰ *S.A.S. c. France* [GC], Requête n° 43835/11, 1er juillet 2014, paragraphe 114 ; *Merabishvili c. Géorgie* [GC], Requête n° 72508/13, 28 novembre 2017, paragraphes 295-296.

pour atteindre le but légitime poursuivi⁸¹. Le critère de nécessité exige que la limitation soit proportionnée au but légitime poursuivi, qu'elle réponde à un besoin social impérieux et qu'elle utilise les moyens les moins restrictifs.

43. Les États devront veiller à ce que toute restriction des droits relatifs de la CEDH ou de la CSE résultant d'activités du cycle de vie des systèmes d'IA satisfasse à toutes ces exigences.

3.1.5 Principales questions relatives aux droits humains dans les secteurs de la gouvernance publique

44. L'utilisation des systèmes d'IA peut avoir un impact sur un éventail de droits humains, certains enjeux apparaissant de manière récurrente dans différents contextes. Il s'agit notamment des risques pour (i) la non-discrimination et l'égalité ; (ii) la protection des données personnelles et de la vie privée ; et (iii) la capacité à contester efficacement les décisions fondées sur l'IA et les voies de recours effectives. Les obligations concurrentes en matière de droits humains dans le contexte de l'IA peuvent également poser problème dans différents secteurs. Ces défis récurrents sont des préoccupations transversales en matière de droits humains dans le cycle de vie des systèmes d'IA et ne se limitent donc pas à un ou plusieurs secteurs publics.

Non-discrimination et égalité

i. L'interdiction de la discrimination

45. La CEDH⁸² et la CSE (révisée)⁸³ elles-mêmes interdisent la discrimination, mais uniquement en ce qui concerne la jouissance des droits et libertés énoncés dans les traités respectifs. De plus, l'article 1 du protocole n° 12 de la CEDH introduit une interdiction plus large de la discrimination, couvrant « tout droit prévu par la loi [nationale] »⁸⁴. Les motifs de discrimination mentionnés dans ces instruments comprennent « le sexe, la race, la couleur, la langue, la religion, les opinions politiques ou toutes autres opinions, l'origine nationale ou sociale, l'appartenance à une minorité nationale, la fortune, la naissance ou toute autre situation ». La notion d'« autre statut » signifie que les motifs énumérés ne sont pas exhaustifs. La Cour a interprété l'expression « autre situation » de manière

⁸¹ *Vavříčka et autres c. République tchèque* [GC], Nos. 47621/13 et 5 autres, 8 avril 2021, paragraphes 273-275 ; *Association internationale Autisme-Europe (AIAE) c. France*, n° 13/2000, 4 novembre 2003, paragraphe 52

⁸² Article 14 de la CEDH.

⁸³ Article E de la CSE. La CSE fait référence à l'interdiction de la discrimination dans son préambule.

⁸⁴ Ce protocole a été ratifié par 20 États membres du Conseil de l'Europe

extensive et à la lumière des conditions actuelles pour y inclure des caractéristiques telles que la nationalité, l'origine ethnique, le sexe, l'orientation sexuelle, l'identité et l'expression de genre, les caractéristiques sexuelles, l'âge, l'état de santé, le handicap, l'état matrimonial, le statut de migrant ou de réfugié⁸⁵. L'interdiction de la discrimination s'applique dans les relations verticales et horizontales. La discrimination peut être directe ou indirecte. La discrimination directe résulte d'une différence de traitement entre « des personnes placées dans des situations analogues ou similaires »⁸⁶ et lorsque cette différence est « fondée sur une caractéristique identifiable ».⁸⁷ La discrimination peut également résulter d'un manquement à traiter différemment des personnes dont la situation est sensiblement différente⁸⁸. Il y a discrimination indirecte lorsque des lois, des politiques ou des pratiques apparemment neutres affectent de manière disproportionnée et injustifiable un groupe particulier de personnes.⁸⁹

46. Le principe d'égalité et de non-discrimination de la Convention-cadre⁹⁰ se réfère au « risque réel et bien documenté de biais pouvant constituer une discrimination illicite découlant des activités menées dans le cadre du cycle de vie des systèmes d'intelligence artificielle »⁹¹, et sa disposition relative à la non-discrimination interdit explicitement la discrimination dans la mise en œuvre de la Convention⁹². Elle s'inspire directement de normes internationales établies, notamment de la CEDH et de la CSE⁹³.

ii. Risques pour la non-discrimination et l'égalité

47. Les systèmes d'IA peuvent présenter des risques pour l'égalité et la non-discrimination, car ils peuvent être construits et soutenus par des données et des modèles qui reproduisent, perpétuent et exacerbent les préjugés, les stéréotypes, la stigmatisation, les préjugés et les fausses hypothèses existants sur les individus, sur la base de caractéristiques personnelles réelles ou perçues et de leurs intersections. Ces effets peuvent être encore aggravés par des asymétries d'information et peuvent être plus sévères pour les personnes en situation de vulnérabilité ou

⁸⁵ Voir le Rapport explicatif de la Recommandation CM/Rec(2024)7 du Comité des Ministres aux États membres sur la protection effective des droits humains dans les situations de crise.

⁸⁶ *Burden c. Royaume-Uni* [GC], n° 13378/05, 29 avril 2008, paragraphe 60.

⁸⁷ *Biao c. Danemark* [GC], n° 38590/10, paragraphe 89.

⁸⁸ *Thlimmenos c. Grèce* [GC], n° 34368/97, 6 avril 2000, paragraphe 44.

⁸⁹ *D.H. et autres c. République tchèque* [GC], n° 57325/00, 13 novembre 2007.

⁹⁰ Convention-cadre, article 10.

⁹¹ Rapport explicatif, paragraphe 75.

⁹² Convention-cadre, article 17.

⁹³ Rapport explicatif, paragraphe 71.

appartenant à des groupes marginalisés. Entre autres, ces effets peuvent entraîner une augmentation de la violence en ligne et hors ligne à l'encontre ces personnes, ainsi qu'à l'encontre des femmes et des filles, qui peuvent être disproportionnellement ciblées en raison des inégalités entre les sexes, des stéréotypes et des déséquilibres de pouvoir existants que les systèmes d'IA peuvent involontairement amplifier⁹⁴.

48. Les systèmes d'IA peuvent être sujets à la discrimination par procuration. Cela signifie que des informations en apparence neutres qui sont indirectement liées à des caractéristiques protégées peuvent dissimuler des préjugés, ce qui rend de plus en plus difficile la traçabilité et la détection d'une discrimination par procuration basée sur l'IA. Par exemple, l'utilisation de données telles que les codes postaux ou les habitudes de consommation peut sembler neutres mais, en tant qu'indicateurs, peuvent refléter indirectement des caractéristiques telles que l'origine ethnique, le genre ou le statut socio-économique, pouvant rendre difficile la traçabilité et la détection d'une discrimination indirecte⁹⁵. Une autre préoccupation concerne la capacité des systèmes d'IA à opérer une discrimination intersectionnelle, c'est-à-dire lorsque plusieurs motifs de discrimination se recoupent⁹⁶.

⁹⁴ Plusieurs instruments juridiques non contraignants ont été adoptés pour lutter contre cette violence, notamment la Recommandation générale n° 1 du Groupe d'experts sur la lutte contre la violence à l'égard des femmes et la violence domestique (GREVIO) sur la dimension numérique de la violence à l'égard des femmes. Le Conseil de l'Europe [a également élaboré] un instrument spécifique sur [la lutte contre] la violence à l'égard des femmes et des filles, facilitée par la technologie.

⁹⁵ D'autres exemples de variables de substitution incluent la pointure de chaussure comme variable de substitution du sexe, les noms comme variable de substitution de l'origine ethnique ou de l'âge, la profession comme variable de substitution du sexe, etc. Voir Fundamental Rights Agency, *Bias in Algorithms – Artificial Intelligence and Discrimination* (2022), p. 24, en anglais uniquement. Pour d'autres exemples, voir le Report of the United Nations Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance A/HRC/56/68 publié le 3 juin 2024, paragraphes 18, 32, 40, (*en anglais uniquement*) ; *Discrimination, intelligence artificielle et prise de décision algorithmique*, Direction générale de la démocratie, 2018 ; Étude sur l'impact des systèmes d'intelligence artificielle, leur potentiel de promotion de l'égalité, y compris l'égalité de genre, et les risques qu'ils peuvent entraîner en matière de non-discrimination, Commission pour l'égalité de genre (GEC) et Comité directeur sur l'anti-discrimination, la diversité et l'inclusion (CDADI) (2023), pp. 17, 56-57, 63, 88.

⁹⁶ Voir l'Étude sur l'impact des systèmes d'intelligence artificielle, leur potentiel de promotion de l'égalité, y compris l'égalité de genre, et les risques qu'ils peuvent entraîner en matière de non-discrimination (2023), p. 67, « En raison de la granularité du profilage algorithmique, les systèmes d'IA sont capables de déduire plusieurs appartenances sociales protégées et de regrouper potentiellement les utilisateurs en fonction de différentes classifications problématiques. Par exemple, les profils algorithmiques peuvent contenir des informations concernant le sexe, l'âge, l'origine ethnique, les croyances religieuses, l'orientation sexuelle ou l'identité de genre, sur la

Le droit à la vie privée et à la protection des données à caractère personnel

i. Le droit à la vie privée et à la protection des données dans la CEDH et dans d'autres instruments pertinents

49. L'article 8 de la CEDH (droit au respect de la vie privée et familiale), par le biais de protection de la vie privée, s'applique à la collecte et au traitement des données à caractère personnel⁹⁷. La vie privée comprend, entre autres, l'image, l'identité, le développement personnel et les relations d'une personne, et s'étend également aux activités professionnelles ou commerciales. Les données à caractère personnel couvrent des informations telles que les noms, les adresses, les adresses IP, ainsi que des données sensibles telles que les informations relatives à la santé et à l'origine ethnique. L'article 8 s'applique également à l'interception de communications, telles que les courriels et les appels téléphoniques. De telles mesures constituent une ingérence dans le droit à la vie privée et toute ingérence de ce type doit être légale, poursuivre un but légitime, être nécessaire et proportionnée.

50. [La Convention n° 108](#)⁹⁸ du Conseil de l'Europe protège les individus en ce qui concerne le traitement automatique des informations à caractère personnel les concernant et constitue le seul traité international juridiquement contraignant traitant exclusivement de cette question.⁹⁹ La Convention n° 108 définit les données à caractère personnel comme « toute information concernant une personne physique identifiée ou identifiable »¹⁰⁰. Les principes clés du traitement des données

base de l'analyse des comportements en ligne, des préférences des consommateur·ices, etc. »

⁹⁷ Pour la jurisprudence de la Cour sur la protection des données personnelles, voir T-PD(2023)1 Jurisprudence sur la protection des données (décembre 2022) et le Guide sur l'article 8 de la Convention européenne des droits de l'homme.

⁹⁸ La Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108). La Convention est modifiée par le Protocole de 2018 (CETS n° 223), qui n'est pas encore en vigueur, qui traite des défis posés à la vie privée par l'utilisation des nouvelles technologies de l'information et de la communication et renforce le mécanisme de la Convention afin d'assurer sa mise en œuvre effective. La Convention 108, telle qu'elle sera modifiée par le Protocole, dès l'entrée en vigueur de ce dernier, est souvent appelée « Convention 108+ ».

⁹⁹ Parmi ceux-ci, les Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontaliers de données à caractère personnel (1980, modifiées en 2013) et le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données/RGPD).

¹⁰⁰ Article 2. Voir également l'article 1 de la Convention 108+, qui stipule que « Le but de la présente Convention est de protéger toute personne physique, quelle que soit sa nationalité ou sa résidence, à l'égard du traitement des données à caractère

personnelles sont la légalité, la nécessité, la proportionnalité, l'équité, la transparence, la limitation des finalités, la minimisation des données, l'exactitude, la sécurité des données, la responsabilité et le contrôle de l'utilisateur sur ses informations. Les personnes doivent être informées de la manière dont leurs données sont collectées et traitées et conserver le droit d'en demander la correction ou l'effacement. Les données à caractère personnel doivent être traitées sur une base juridique valable et à des fins légitimes présélectionnées. La Cour s'est référée à de nombreuses occasions aux normes de la Convention n° 108 dans ses arrêts concernant la protection des données.¹⁰¹

51. La protection des droits à la vie privée et des données à caractère personnel est un principe commun nécessaire à la mise en œuvre effective de nombreux autres principes de la Convention-cadre.¹⁰² La Convention-cadre oblige les parties à adopter ou à maintenir des mesures garantissant la protection de la vie privée et des données à caractère personnel tout au long du cycle de vie des systèmes d'IA¹⁰³. Il s'agit notamment de se conformer aux lois nationales et internationales applicables, telles que la CEDH et la Convention n° 108¹⁰⁴. D'autres instruments du Conseil de l'Europe soulignent également la nécessité de mettre en place des garanties efficaces pour faire face aux risques liés à la vie privée et à la protection des données qui découlent de l'utilisation des systèmes d'IA¹⁰⁵.

personnel, contribuant ainsi au respect de ses droits de l'homme et de ses libertés fondamentales et notamment du droit à la vie privée. »

¹⁰¹ *Z. c. Finlande*, n° 22009/93, 25 février 1997 paragraphe 95, ; *Amann c. Suisse* [GC], n° 27798/95, 16 février 2000, paragraphe 65 ; *Rotaru c. Roumanie* [GC], n° 28341/95, 4 mai 2000, paragraphe 43 ; *P.G. et J.H. c. Royaume-Uni*, n° 44787/98, 25 décembre 2001, paragraphe 57 ; *Sofianopoulos et autres c. la Grèce* (déc.), n° 1977/02, 1988/02 et 1997/02, 16 février 2000 ; *Peck c. Royaume-Uni*, n° 44647/98, 28 avril 2003, paragraphe 78, ; *Von Hannover c. Allemagne*, n° 59320/00, 24 septembre 2004, paragraphe 42 ; *Cemalettin Canlı c. Turquie*, n° 22427/04, 18 février 2009, paragraphes 17 et 34 ; *S. et Marper c. Royaume-Uni*, n° 30562/04 et 30566/04, 4 décembre 2008, paragraphes 41, 66, 68, 76, 103, 104 et 107 ; *Uzun c. Allemagne*, n° 35623/05, 2 septembre 2010, paragraphe 47.

¹⁰² Convention-cadre, Rapport explicatif, paragraphe 79.

¹⁰³ Convention-cadre, Article 11.

¹⁰⁴ Rapport explicatif, paragraphes 80-83.

¹⁰⁵ Voir les Lignes directrices 2019 sur l'intelligence artificielle et la protection des données adoptées par le Comité consultatif de la Convention 108 ; la Recommandation CM/Rec(2020)1 du Comité des Ministres aux États membres sur les impacts des systèmes algorithmiques sur les droits de l'homme ; La recommandation CM/Rec(2021)8 du Comité des ministres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage souligne le droit des personnes à s'opposer au profilage et exige des garanties solides, en particulier lorsque le profilage affecte de manière significative leurs droits.

ii. Risques liés à la protection de la vie privée et des données

52. Les systèmes d'IA peuvent présenter des risques importants pour la vie privée et la protection des données, notamment en raison de leur dépendance à l'égard de grands volumes de données à caractère personnel à des fins de formation et d'exploitation. Les systèmes d'IA collectent, analysent et déduisent souvent des informations sensibles, parfois à l'insu des personnes concernées, ce qui soulève des questions quant à la validité de la base juridique, à la minimisation des données et à la limitation des finalités. L'utilisation de l'IA dans des domaines tels que la publicité ciblée, la surveillance des réseaux sociaux et l'identification biométrique peut conduire à une surveillance omniprésente, y compris une surveillance de masse et un profilage, susceptibles de porter atteinte aux droits des individus à la vie privée et à l'autonomie.

53. Parmi les risques supplémentaires figurent le risque d'exposition des données à caractère personnel par le biais de la réidentification et des fuites de données. Lorsque les données à caractère personnel sont traitées par des modèles opaques ou complexes, il devient difficile d'évaluer comment les données sont utilisées ou si les droits des personnes sont respectés. Ce manque de transparence nuit à la responsabilité et rend plus difficile pour les individus d'exercer leurs droits en vertu des lois sur la protection des données, tels que l'accès, la correction ou la suppression de leurs données, ou la nouvelle génération de droits des personnes concernées. Ces risques sont amplifiés et peuvent avoir de graves répercussions sur les droits humains dans des contextes tels que l'application de la loi ou le contrôle des frontières¹⁰⁶.

Des recours effectifs

i. Le droit à un recours effectif dans la CEDH, la CSE et autres instruments pertinents

54. L'article 13 de la CEDH garantit à toute personne le droit à un recours effectif en cas de violation des droits et libertés qui lui sont reconnus par la CEDH. Les recours doivent être disponibles, accessibles et abordables, efficaces tant en droit qu'en pratique, et capables de traiter le fond de la violation alléguée et de fournir une réparation appropriée¹⁰⁷.

¹⁰⁶ Adopté par le Comité consultatif de la Convention 108.

¹⁰⁷ *Boyle et Rice c. Royaume-Uni*, 27 avril 1988, n° 9659/82 et 9658/82, paragraphe 52 ; *Powell et Rayner c. Royaume-Uni*, 21 février 1990, paragraphe 31 ; *M.S.S. c. Belgique et Grèce* [GC], n° 30696/09, 21 janvier 2011, paragraphe 288 ; *De Souza Ribeiro c. France* [GC], 2012, n° 22689/07, 13 décembre 2012, paragraphe 78 ; *Centre for Legal Resources au nom de Valentin Câmpeanu c. Roumanie* [GC], 17 juillet 2014, paragraphe 148. *Paulino Tomás v. Portugal*, (dec), n° 58698/00.

Ils peuvent inclure des mécanismes judiciaires ou un organisme quasi judiciaire tel qu'une institution de l'Ombudsman¹⁰⁸, ou une autorité politique telle qu'une commission parlementaire¹⁰⁹. S'ils ne sont pas portés devant une autorité judiciaire, ils doivent néanmoins être indépendants et des garanties procédurales doivent être offertes au requérant¹¹⁰. Dans certaines circonstances, cependant, un recours devant une autorité judiciaire peut être essentiel (par exemple concernant la révision et la supervision des mesures de surveillance secrètes) ou souhaitable¹¹¹. Les obligations positives des États¹¹² peuvent les amener à fournir un recours effectif également en ce qui concerne les violations des droits de l'homme par des acteurs privés, y compris les entreprises¹¹³.

55. La CSE ne prévoit pas explicitement le droit à un recours effectif, mais la CSE (révisée) a interprété la CSE comme exigeant un recours effectif dans certains cas.

56. Conformément à son article 9, les parties à la Convention-cadre sont tenues d'adopter de nouveaux cadres ou mécanismes ou de maintenir ceux qui existent déjà afin que tous les acteurs responsables d'activités dans le cycle de vie des systèmes d'IA, qu'il s'agisse d'organisations publiques ou privées, soient tenus de rendre compte des effets négatifs sur les droits humains, la démocratie et l'État de droit résultant de ces activités. Cela peut inclure des mesures judiciaires et administratives, des régimes de responsabilité civile, pénale et autre et, dans le secteur public, des procédures administratives et autres permettant de contester les décisions, ou l'attribution de responsabilités spécifiques aux opérateurs¹¹⁴. En outre, les Parties à la Convention-cadre sont tenues d'adopter ou de maintenir des mesures visant à garantir la disponibilité de recours accessibles et efficaces, dans la mesure où ces recours sont requis par les obligations des Parties en cas de violations

¹⁰⁸ *Leander c. Suède* (n° 9248/81, 26 mars 1987)

¹⁰⁹ *Klass et autres c. Allemagne*, n° 5029/71, 6 septembre 1978, paragraphe 67.

¹¹⁰ *Khan c. Royaume-Uni*, n° 35394/97, 12 mai 2000, paragraphes 44-47.

¹¹¹ Voir par exemple *Big Brother Watch et autres c. Royaume-Uni* [GC], n° 58170/13, 62322/14 et 24960/15, 25 mai 2021, paragraphe 336 : « Dans un domaine où les abus dans des cas individuels sont potentiellement si faciles et pourraient avoir des conséquences aussi néfastes pour la société démocratique dans son ensemble, la Cour a estimé qu'il est en principe souhaitable de confier le contrôle de la surveillance à un juge, le contrôle judiciaire offrant les meilleures garanties d'indépendance, d'impartialité et de procédure régulière ». Voir également *Ramirez Sanchez c. France* [GC], n° 59450/00, 4 juillet 2006, paragraphes 165-166 ; *Danilczuk c. Chypre*, n° 21318/12, 3 avril 2018, paragraphes 44.

¹¹² En ce qui concerne les obligations positives, voir ci-dessous, section 3.2.1

¹¹³ *Z et autres c. Royaume-Uni* [GC], n° 29392/95, 10 mai 2001, paragraphe 109 ; *Keenan c. Royaume-Uni*, n° 27229/95, 3 avril 2001, paragraphe 129 ; *Paul et Audrey Edwards c. Royaume-Uni*, n° 46477/99, 14 juin 2002, paragraphe 97.

¹¹⁴ Rapport explicatif, paragraphes 66-68.

des droits humains résultant d'activités menées dans le cadre du cycle de vie des systèmes d'IA¹¹⁵.

ii. Risques pour le droit à un recours effectif

57. L'exercice du droit à un recours effectif peut être entravé dans le cas de violations présumées liées aux systèmes d'IA en raison du manque de transparence et d'explicabilité concernant l'utilisation de ces systèmes, de leur complexité technique, de leur opacité et de leur dépendance à l'égard de vastes ensembles de données et de divers acteurs en amont de la chaîne d'approvisionnement. Les individus peuvent ne pas avoir les connaissances ou l'accès aux informations nécessaires pour identifier les violations et la personne ou l'entité responsable. Ils peuvent également ne pas être conscients de l'ampleur des atteintes à leurs droits ou avoir du mal à comprendre les processus décisionnels sous-jacents. Comme indiqué ci-dessus, les recours doivent être accessibles - disponibles et compréhensibles pour les individus - et efficaces, c'est-à-dire qu'ils doivent permettre de manière adéquate les violations des droits humains liées aux systèmes d'IA et d'offrir une réparation.

58. De plus, une dépendance excessive à l'égard de l'IA peut entraîner un transfert involontaire de responsabilité vers le système lui-même, créant ainsi des lacunes en matière de responsabilité. En l'absence de cadres juridiques ou de mécanismes de contrôle clairs, les individus peuvent se heurter à des obstacles pour accéder à la justice, notamment des retards, un manque d'informations ou des processus de révision inadéquats.

3.2 Entreprises et droits humains

59. Cette section explore l'intersection entre les activités commerciales liées à l'IA et les obligations en matière de droits humains, en se concentrant sur les obligations positives des États en vertu de la CEDH et de la CSE, sur l'équilibre entre les droits humains des entreprises et ceux des individus, et sur la responsabilité des entreprises de respecter les droits humains dans le cadre plus large des normes internationales non contraignantes.

¹¹⁵ Convention-cadre, article 14. Cela comprend la documentation et la mise à disposition des informations pertinentes, le cas échéant et lorsque cela est applicable, aux personnes concernées, afin de leur permettre de comprendre et d'exercer leurs droits. Voir la Convention-cadre, rapport explicatif, paragraphe 99.

3.2.1 Obligations positives en vertu de la CEDH et de la CSE¹¹⁶

60. La CEDH et la CSE n'imposent pas directement d'obligations en matière de droits humains aux entreprises qui n'exercent pas de fonction publique. Si les particuliers ne peuvent pas porter plainte directement contre des entreprises devant la Cour ou le CEDS, ils peuvent, en fonction du droit lésé, intenter des actions contre les États qui n'ont pas empêché ou traité les abus résultant d'activités liées aux entreprises.

61. En vertu de la CEDH et de la jurisprudence de la Cour, les États pourraient, par exemple, être tenus pour responsables lorsqu'ils tolèrent ou ferment les yeux sur des actes d'acteurs privés qui violent les droits humains¹¹⁷ ou lorsqu'ils ne réglementent pas correctement le secteur privé¹¹⁸. La portée et le contenu concrets des obligations des États développées par la jurisprudence de la Cour en matière de prévention et de réparation des violations des droits humains liées aux entreprises dépendent dans une certaine mesure du droit humain en question et des circonstances factuelles. En général, les obligations positives consistent à prévenir les violations des droits humains lorsque les autorités compétentes ont eu connaissance ou auraient dû avoir connaissance d'un risque réel de telles violations ; à mener une enquête officielle indépendante et impartiale, adéquate et rapide lorsque de telles violations sont présumées avoir eu lieu ; à engager des poursuites efficaces et à prendre toutes les mesures appropriées pour mettre en place des mécanismes accessibles et efficaces exigeant que les victimes de telles violations reçoivent une réparation rapide et adéquate pour tout préjudice subi¹¹⁹. Le fait de ne pas avoir pris les mesures raisonnablement disponibles qui auraient pu avoir une chance réelle de modifier le résultat ou d'atténuer le préjudice suffit à engager la responsabilité de l'État¹²⁰.

¹¹⁶ Il est également possible que les États manquent à leurs obligations négatives, dans les cas où les violations des droits humains liées aux entreprises sont imputables à l'État. Cela pourrait se produire, par exemple, lorsqu'une entreprise est détenue ou contrôlée par l'État, ou lorsqu'une entreprise agit en tant qu'agent de l'État. Néanmoins, le présent Manuel se concentre sur les obligations positives, étant donné qu'à l'heure actuelle, les activités pertinentes dans le cycle de vie des systèmes d'IA sont largement menées par le secteur privé.

¹¹⁷ *Ilaşcu et autres c. Moldova et Russie* [GC], n° 48787/99, 8 juillet 2004, paragraphe 318.

¹¹⁸ *Hatton et autres c. Royaume-Uni* [GC], n° 30622/1997, 8 juillet 2003, paragraphe 98.

¹¹⁹ Recommandation CM/Rec(2016)3 du Comité des Ministres sur les droits de l'homme et les entreprises, paragraphe 15.

¹²⁰ *E. et autres c. Royaume-Uni*, n° 33218/96, 26 novembre 2002, paragraphes 99-100.

62. La CSE offre également une protection contre les violations des droits humains liées aux activités commerciales, en particulier en ce qui concerne les droits des travailleurs. Dans le cadre de leur politique, les États membres devraient prendre toutes les mesures nationales et internationales appropriées pour assurer la réalisation effective des droits et principes de la CSE et envisager d'accepter des dispositions supplémentaires¹²¹.

63. Des obligations positives au titre de la CEDH peuvent se présenter dans un large éventail de situations, telles que l'ingérence des entreprises de médias dans la liberté d'expression¹²² ; les abus dans les hôpitaux¹²³ et les écoles privés¹²⁴ ; les restrictions vestimentaires sur le lieu de travail affectant le droit de manifester sa religion¹²⁵ ; la fourniture aux travailleurs d'informations permettant d'évaluer les risques pour la santé et la sécurité au travail¹²⁶ ; ou les atteintes aux droits humains liées à l'environnement causées par les activités des entreprises¹²⁷. En vertu de la CSE, des obligations positives peuvent, par exemple, découler du droit à la santé en vertu de l'article 11¹²⁸, de la prévention du travail forcé et d'autres formes d'exploitation par le travail¹²⁹, ou de la prise de mesures préventives appropriées (campagnes d'information, de sensibilisation et de prévention sur le lieu de travail ou en relation avec le travail) afin de lutter contre le harcèlement moral¹³⁰.

¹²¹ Recommandation CM/Rec(2016)3 sur les droits de l'homme et les entreprises, paragraphe 16 ; voir également *Marangopoulos Foundation for Human Rights (MFHR) c. Grèce*, réclamation n° 30/2005, décision sur la recevabilité du 10 octobre 2005, paragraphe 14, le CEDS a décidé que l'État est responsable de l'application des droits inscrits dans la Charte dans sa juridiction, même si l'État n'a pas agi en tant qu'opérateur mais a simplement omis de mettre fin aux violations alléguées en sa qualité de régulateur. Dans l'Interprétation de l'article 17 paragraphe 2 – Participation du secteur privé à l'éducation, Conclusions 2019, les États parties sont tenus de réglementer et de superviser strictement la participation du secteur privé à l'éducation, en veillant à ce que le droit à l'éducation ne soit pas compromis.

¹²² *Von Hannover c. Allemagne* [n° 2] [GC], n° 40660/08 et 60641/08, 7 février 2012.

¹²³ *Storck c. Allemagne*, n° 61603/00, 16 juin 2005.

¹²⁴ *Costello-Roberts c. Royaume-Uni*, n° 13134/87, 25 mars 1993.

¹²⁵ *Eweida et autres c. Royaume-Uni*, n° 48420/10 et 3 autres, 27 mai 2013.

¹²⁶ *Vilnes et autres c. Norvège*, n° 52806/09 et 22703/10, 24 mars 2014.

¹²⁷ *Lopez Ostra c. Espagne*, n° 16798/90, 9 décembre 1994 ; *Guerra et autres c. Italie* [GC], n° 116/1996/735/932, 19 février 1998, 19 février 1998, paragraphe 58 ; *Taşkin et autres c. Turquie*, n° 46117/99, 30 mars 2005 ; *Fadeyeva c. Russie*, n° 55723/00, 9 juin 2005, paragraphe 89.

¹²⁸ CSER, Conclusions 2005 - Déclaration interprétative - Article 11.

¹²⁹ CSER, Conclusions 2020, Albanie.

¹³⁰ CSER, Conclusions 2014, Azerbaïdjan ; Conclusions 2005, République de Moldova.

64. La jurisprudence de la Cour, dans des circonstances spécifiques, met en évidence (i) les obligations positives de réglementer et de contrôler les opérations commerciales ; (ii) les obligations procédurales positives de permettre la participation du public et la prise de décisions en connaissance de cause ; et (iii) les obligations positives de fournir des recours efficaces en cas de violations des droits humains liées aux entreprises. En ce qui concerne les obligations positives au titre des droits économiques, sociaux et culturels, le Comité européen des droits sociaux a examiné les obligations des États de réglementer et de superviser le comportement des acteurs privés en matière d'environnement¹³¹, d'éducation¹³² et d'énergie¹³³. Le Comité européen des droits sociaux a souligné que la participation du secteur privé aux services liés aux droits économiques, sociaux et culturels ne doit pas compromettre la jouissance ou la réalisation de ces droits¹³⁴.

Obligations de réglementer et de surveiller les activités des entreprises

65. Dans le cadre de leurs obligations positives telles qu'expliquées précédemment, les États ont le devoir de protéger contre les violations des droits humains commises par des tiers, y compris des entreprises commerciales, et de prendre des mesures raisonnables et appropriées pour garantir les droits fondamentaux des individus. En fonction des circonstances et du contexte spécifique de chaque affaire, les questions qui se posent sont notamment de savoir si l'on pouvait raisonnablement attendre des autorités nationales qu'elles agissent de manière à prévenir ou à mettre fin à la violation alléguée¹³⁵, et si elles ont pris les mesures nécessaires pour assurer la protection effective des droits des requérants¹³⁶. Les États ont l'obligation d'assurer une protection contre les violations des droits humains commises par des tiers, y compris des entreprises commerciales, au moyen d'obligations contraignantes en

¹³¹ *Fondation Marangopoulos pour les droits de l'homme (MFHR) c. Grèce*, plainte n° 30/2005, décision sur la recevabilité du 10 octobre 2005, paragraphe 14.

¹³² Conclusions 2019, Déclaration interprétative sur l'article 17 paragraphe 2 – Participation du secteur privé à l'éducation.

¹³³ *Defence for Children International (DCI), European Federation of National Organisations working with the Homeless (FEANTSA), Magistrats Européens pour la Démocratie et les Libertés (MEDEL), Confederación Sindical de Comisiones Obreras (CCOO) et International Movement ATD Fourth World c. Espagne*, plainte n° 206/2022, décision sur le fond du 11 septembre 2024, paragraphes 55-57.

¹³⁴ *Defence for Children International (DCI), European Federation of National Organisations working with the Homeless (FEANTSA), Magistrats Européens pour la Démocratie et les Libertés (MEDEL), Confederación Sindical de Comisiones Obreras (CCOO) and International Movement ATD Fourth World c. Espagne*, plainte n° 206/2022, décision sur le fond du 11 septembre 2024, paragraphe 57.

¹³⁵ *Fadeyeva v. Russie*, n° 55723/00, 9 juin 2005, paragraphe 89.

¹³⁶ *López Ostra v. Espagne*, paragraphe 55 ; *Guerra et autres v. Italie*, paragraphe 58.

matière de diligence raisonnable en matière de droits humains, de réglementations efficaces et de mécanismes de contrôle tout au long du cycle de vie de l'IA.

66. Les États responsables peuvent également être tenus responsables de leur manquement à informer le public des risques liés à des activités dangereuses et à émettre des avertissements.¹³⁷ Dans le cadre des articles 8 (droit au respect de la vie privée et familiale) et 2 (droit à la vie), il existe une obligation de fournir au public des informations essentielles sur les activités dangereuses liées à l'activité commerciale¹³⁸. En outre, le droit du public à l'information ne doit pas se limiter aux risques qui se sont déjà matérialisés, mais doit figurer parmi les mesures préventives à prendre.¹³⁹

67. Les États devraient examiner si les entreprises impliquées dans le cycle de vie de l'IA sont soumises à une surveillance adéquate. La question de savoir si « l'on peut raisonnablement attendre de l'État qu'il agisse de manière à prévenir ou à mettre fin à la violation alléguée des droits du demandeur » pourrait s'appliquer aux manquements de l'État à traiter, par exemple, les « biais algorithmiques » ou les processus décisionnels opaques de l'IA.

Obligations procédurales positives pour permettre la participation du public et une prise de décision en connaissance de cause

68. Les décisions de l'État relatives aux activités commerciales - telles que l'octroi d'une licence - peuvent également avoir une incidence sur les droits humains. Il convient donc d'évaluer les risques et les répercussions potentielles avant de prendre une décision. Les processus décisionnels « concernant des questions d'impact culturel, environnemental et économique [...] doivent nécessairement faire l'objet d'enquêtes et d'études appropriées afin de permettre [aux autorités publiques] de trouver un juste équilibre entre les différents intérêts contradictoires en jeu »¹⁴⁰. Afin de respecter les intérêts protégés par l'article 8 de la CEDH, par exemple, le processus décisionnel conduisant à des mesures d'ingérence doit « prendre en considération tous les aspects procéduraux, y compris le type de politique ou de décision en cause, la mesure dans laquelle les opinions des individus ont été prises en compte tout au long du processus

¹³⁷ *Tătar c. Roumanie*, requête n° 67021/01, 27 janvier 2009, paragraphes 113-116, 121-124.

¹³⁸ *Vilnes et autres c. Norvège*, n°s 52806/09 et 22703/10, 24 mars 2014, paragraphe 235 ; *Roche c. Royaume-Uni* [GC], n° 32555/96, 19 octobre 2005 paragraphe 162.

¹³⁹ *Vilnes et autres c. Norvège*, n° 52806/09 et 22703/10, 24 mars 2014, paragraphe 235.

¹⁴⁰ *Zammit Maempel c. Malte*, requête n° 24202/10, 22 novembre 2011, paragraphe 62 (*en anglais uniquement ; traduction libre*).

décisionnel et les garanties procédurales disponibles. »¹⁴¹ Dans les affaires environnementales, cela nécessite des enquêtes et des études « de manière à prévenir et évaluer à l'avance les effets des activités qui peuvent porter atteinte à l'environnement et aux droits des individus ». ¹⁴² La réglementation nationale « par ailleurs prévoir des procédures adéquates tenant compte des aspects techniques de l'activité en question et permettant de déterminer ses défaillances ainsi que les fautes qui pourraient être commises à cet égard par les responsables à différents échelons »¹⁴³.

69. Dans la Convention-cadre, les principes de transparence et de contrôle¹⁴⁴ exigent « l'ouverture et la clarté dans la gouvernance des activités menées dans le cadre du cycle de vie des systèmes d'intelligence artificielle et signifie spécifiquement que les processus décisionnels et le fonctionnement général des modèles d'intelligence artificielle devraient être compréhensibles et accessibles aux acteurs appropriés de l'intelligence artificielle et, le cas échéant, aux parties prenantes concernées. »¹⁴⁵

70. Afin de garantir le plein exercice des droits humains et des libertés démocratiques, la Recommandation [CM/Rec\(2020\)1](#) du Comité des Ministres aux États membres sur les impacts des systèmes algorithmiques sur les droits de l'homme recommande aux États de sensibiliser le grand public aux capacités, aux pouvoirs et aux conséquences des systèmes algorithmiques, y compris leur utilisation potentielle pour manipuler, exploiter, tromper ou distribuer des ressources, en vue de permettre à tous les individus et groupes de connaître leurs droits et de savoir comment les mettre en pratique, ainsi que d'utiliser les technologies numériques à leur avantage. En outre, tous les acteurs concernés, y compris ceux des secteurs public, privé et de la société civile dans lesquels des systèmes algorithmiques sont envisagés ou utilisés, devraient promouvoir, encourager et soutenir de manière adaptée et inclusive (en tenant compte de la diversité en ce qui concerne, par exemple, l'âge, le genre, la race, l'origine ethnique, le contexte culturel ou socio-économique) un niveau de maîtrise des médias, du numérique et de l'information qui permette une prise en compte et une utilisation compétentes et critiques des systèmes algorithmiques.¹⁴⁶

¹⁴¹ *Taskin et autres c. Turquie*, paragraphe 118.

¹⁴² Idem.

¹⁴³ *Öneryıldız c. Turquie* [GC], paragraphe 90.

¹⁴⁴ Voir l'article 8 de la Convention-cadre.

¹⁴⁵ Rapport explicatif, paragraphe 57.

¹⁴⁶ Recommandation CM/Rec(2020)1 du Comité des Ministres aux États membres sur les impacts des systèmes algorithmiques sur les droits de l'homme, section B, paragraphe 1.3.

Obligations relatives à la mise en place de voies de recours effectives

71. Les États peuvent être tenus de fournir des recours efficaces pour les violations des droits humains liées aux entreprises. Cela peut inclure la modification des lois si le cadre juridique est inadéquat¹⁴⁷ et la garantie que les entreprises respectent le droit national. Le droit à un recours effectif (article 13 de la CEDH) est pertinent à cet égard.

Marge d'appréciation dans le cadre des obligations positives

72. Il est important de noter que les États jouissent généralement d'une large marge d'appréciation pour décider de la manière de remplir leurs obligations en ce qui concerne les activités commerciales susceptibles d'avoir un impact sur les droits humains. Cette marge d'appréciation interprétée par la Cour se réduit toutefois si les mesures prises par l'État interfèrent avec un aspect des plus intimes de la vie privée d'une personne¹⁴⁸, en fonction de la gravité des menaces pesant sur le droit en question.¹⁴⁹ De plus, il incombe à l'État de justifier, à l'aide de données détaillées et rigoureuses, une situation dans laquelle des individus supportent un lourd fardeau au nom du reste de la communauté¹⁵⁰.

73. Ainsi, même si une marge d'appréciation est attendue dans la réglementation des technologies d'IA dans le cadre des activités commerciales, celle-ci pourrait être considérablement limitée lorsque les systèmes d'IA présentent des risques graves pour les droits humains.

3.2.2 Équilibrer les droits des entreprises dans le contexte de la gouvernance de l'IA

74. Les exigences de transparence et d'explicabilité concernant, par exemple, l'atténuation des préjugés soulèvent des questions relatives à l'intersection des droits des individus et des lois sur la propriété intellectuelle et les secrets d'affaires. Le système d'IA d'une entreprise peut être couvert par la législation sur la propriété intellectuelle et les secrets commerciaux. De plus, les entreprises ont également droit à la protection des droits humains spécifiques en vertu de la CEDH, tels que

¹⁴⁷ *Fadeyeva c. Russie*, paragraphes 89 et 92 ; voir aussi *Powell et Rayner c. Royaume-Uni*, n° 93101/81, 21 février 1990.

¹⁴⁸ *Hatton & autres c. Royaume-Uni* [GC], 7 août 2003, paragraphe 102.

¹⁴⁹ *Brincat et autres c. Malte*, requête n° 60908/11 et al., 24 juillet 2014, paragraphe 116.

¹⁵⁰ *Dubetska et autres c. Ukraine*, requête n° 30499/03, 10 février 2011, paragraphe 145.

les droits de propriété (Article 1 du protocole 1 CEDH qui inclut la propriété intellectuelle)¹⁵¹ ou la liberté d'expression (article 10 de la CEDH).¹⁵²

75. Si les détenteurs de droits affirment que les systèmes d'IA exploités par des entreprises privées portent atteinte à leurs droits, la réponse de l'État devra peut-être trouver un équilibre entre ces intérêts concurrents. Par exemple, l'obligation de fournir des informations essentielles au public peut entrer en conflit avec les droits de propriété intellectuelle d'une entreprise (protégés par le droit de propriété - article 1 du protocole 1 de la CEDH). Les tribunaux nationaux ou les régulateurs nationaux doivent soigneusement peser ces intérêts afin de garantir un résultat juste et proportionnel.

76. Les rédacteurs de la Convention-cadre ont noté, en ce qui concerne le principe de transparence (article 8 de la Convention-cadre), que « les Parties sont tenues, dans la mise en œuvre de ce principe, de trouver un juste équilibre entre les divers intérêts concurrents et de procéder aux ajustements nécessaires dans les cadres pertinents sans altérer ou modifier fondamentalement le régime sous-jacent des droits de l'homme applicables ». ¹⁵³

77. Dans le contexte des systèmes algorithmiques, la [recommandation CM/Rec\(2020\)1 du Conseil de l'Europe sur les impacts des systèmes algorithmiques sur les droits de l'homme](#) prévoit que les cadres législatifs relatifs à la propriété intellectuelle ou aux secrets commerciaux ne doivent pas empêcher la transparence ou être exploités pour faire obstacle à la responsabilité, et que la confidentialité ou les secrets commerciaux ne doivent pas entraver la réalisation d'évaluations efficaces de l'impact sur les droits humains¹⁵⁴. De plus, les États devraient établir des niveaux de transparence appropriés en ce qui concerne les critères et méthodes de passation de marchés publics, d'utilisation, de conception et de traitement de base des systèmes algorithmiques mis en œuvre par et pour eux, ou par des acteurs du secteur privé¹⁵⁵.

¹⁵¹ *Anheuser-Busch Inc. c. Portugal* [GC], n° 73049/01, 11 janvier 2007, paragraphe 72.

¹⁵² *Axel Springer AG c. Allemagne* [GC], n° 39954/08, arrêt du 7 février 2012.

¹⁵³ Convention-cadre, Rapport explicatif, paragraphe 62.

¹⁵⁴ CM/Rec(2020)1, paragraphe 5.2.

¹⁵⁵ *Idem*, paragraphe 4.1 Les niveaux de transparence en question devraient être aussi élevés que possible et proportionnels à la gravité des incidences négatives sur les droits humains. L'utilisation de tels systèmes dans les processus décisionnels qui comportent un risque élevé pour les droits humains devrait être soumise à des normes particulièrement élevées.

3.2.3 Principaux cadres non contraignants sur les entreprises, les droits humains et l'IA

Instruments non contraignants pertinents

78. Les Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme (UNGP) font partie des cadres de gouvernance mondiaux et régionaux pertinents. Ces principes directeurs prévoient une série de principes que les États et les entreprises devraient appliquer ou envisager d'appliquer (selon les circonstances), en utilisant le cadre « Protéger, respecter et réparer » : (i) le devoir de l'État de protéger contre les abus, (ii) la responsabilité des entreprises de respecter les droits humains et (iii) l'accès à des voies de recours pour les victimes.

79. S'appuyant sur les principes directeurs des Nations unies, le Comité des ministres du Conseil de l'Europe a adopté la [recommandation CM/Rec\(2016\)3 sur les droits de l'homme et les entreprises](#). Elle fournit des orientations spécifiques pour aider les États membres à prévenir les violations des droits humains par les entreprises et à y remédier, et insiste sur les mesures visant à inciter les entreprises à respecter les droits humains.

80. Les Principes directeurs de l'OCDE à l'intention des entreprises multinationales sur la conduite responsable des entreprises, qui fournissent des recommandations détaillées sur la conduite responsable des entreprises adressées par les gouvernements aux entreprises multinationales, constituent un autre instrument pertinent.

81. L'obligation des États membres du Conseil de l'Europe de protéger contre les violations des droits humains liées aux activités des entreprises et de fournir des recours efficaces est illustrée au mieux par la jurisprudence de la Cour et les décisions et les conclusions du CEDS, comme indiqué ci-dessus. Les responsabilités des entreprises en matière de respect des droits humains dans le contexte de l'IA peuvent être examinées à travers le prisme des Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme, comme expliqué ci-dessous.

Responsabilité des entreprises en matière de respect des droits humains

82. Les Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme préconisent que les entreprises mettent en place des politiques et des processus, notamment (i) des engagements politiques pour assumer leur responsabilité en matière de respect des droits humains ; (ii) une diligence raisonnable en matière de droits

humains pour identifier, prévenir et traiter les impacts négatifs sur les droits humains ; (iii) des processus permettant de remédier à leurs impacts négatifs sur les droits humains¹⁵⁶. Les entreprises doivent utiliser des indicateurs qualitatifs et quantitatifs, intégrer ce suivi dans les processus internes et solliciter le retour d'information des parties prenantes (principe 20). Lorsque les entreprises causent ou contribuent à des impacts négatifs, elles doivent mettre en place des mesures correctives ou coopérer à leur mise en œuvre par le biais de processus légitimes (principe 22). Si les impacts sont liés aux activités de l'entreprise mais ne sont pas directement causés par elle, l'entreprise n'est pas tenue d'y remédier elle-même mais peut jouer un rôle de soutien dans le cadre d'efforts plus larges. Lorsqu'il est nécessaire d'établir un ordre de priorité, les entreprises doivent se concentrer en premier lieu sur les impacts les plus graves ou irrémédiables afin de minimiser les dommages (principe 24). La communication sur ces mesures doit être transparente et accessible, en conciliant les préoccupations légitimes de confidentialité et la nécessité de rendre des comptes (principe 21).

83. À ce jour, aucune directive générale spécifique à l'IA n'a été élaborée concernant la responsabilité des entreprises en matière de droits humains¹⁵⁷. Les Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme peuvent toutefois fournir un cadre permettant d'aborder les incidences sur les droits humains tout au long de la chaîne de valeur de l'IA. Les entreprises doivent évaluer et atténuer les risques en matière de droits humains tout au long du cycle de vie de l'IA, de la conception au déploiement, en plaçant la transparence et la responsabilité au cœur de leurs principes. La diligence raisonnable en matière de droits humains devrait évaluer les impacts directs et indirects, en se concentrant sur les risques pour les individus, et devrait être adaptée de manière dynamique à la nature évolutive des technologies de l'IA. Il conviendrait sans doute d'élaborer et d'appliquer des évaluations d'impact sur les droits humains spécifiques à l'IA afin d'identifier les risques en matière de droits humains, y compris ceux découlant de l'utilisation de systèmes d'IA par des tiers.

¹⁵⁶ Principes directeurs des Nations Unies, principes 15-24.

¹⁵⁷ L'OCDE élabore actuellement des lignes directrices sur la diligence raisonnable en matière de conduite responsable des entreprises dans le développement et l'utilisation de systèmes d'IA fiables. En outre, le projet B-Tech des Nations unies sur les droits humains a identifié trois grands thèmes et formulé des recommandations pratiques sur la manière dont les législateurs, les organismes de normalisation, les entreprises et la société civile peuvent tirer parti des Principes directeurs des Nations unies pour promouvoir une gouvernance et des pratiques commerciales capables de faire face aux impacts et aux risques de l'IA générative sur les droits humains (voir *Advancing Responsible Development and Deployment of Generative AI: A UN B-Tech foundational paper* | OHCHR).

84. Dans le contexte spécifique de l'IA, la [méthodologie HUDERIA](#)¹⁵⁸, bien qu'elle ne soit pas un instrument spécifique sur la responsabilité des entreprises en matière de respect des droits humains, s'adresse aux acteurs publics et privés. Elle relie les normes internationales en matière de droits humains et les cadres techniques existants sur la gestion des risques dans le contexte de l'IA et fournit une approche structurée de l'évaluation des risques et des impacts des systèmes d'IA spécifiquement adaptée à la protection et à la promotion des droits de l'homme, de la démocratie et de l'État de droit.

85. La [Recommandation CM/Rec\(2016\)3 sur les droits de l'homme et les entreprises](#) invite les États membres à appliquer les mesures nécessaires pour encourager ou, le cas échéant, exiger que les entreprises domiciliées sur leur territoire ayant des activités dans le cycle de vie de l'IA appliquent une diligence raisonnable en matière de droits humains tout au long de leurs opérations et effectuent une diligence raisonnable en matière de droits humains en ce qui concerne ces activités, y compris des évaluations de l'impact sur les droits humains spécifiques au projet, en fonction de la taille de l'entreprise et de la nature et du contexte de l'opération¹⁵⁹. Les États devraient encourager et, le cas échéant, exiger de ces entreprises qu'elles fassent preuve d'une plus grande transparence afin de leur permettre de mieux « connaître et montrer » leur responsabilité d'entreprise en matière de respect des droits humains et, le cas échéant, exiger de ces entreprises qu'elles fournissent régulièrement, ou en tant que de besoin, des informations sur leurs efforts en matière de responsabilité d'entreprise en matière de respect des droits de humains dans le contexte de l'IA.¹⁶⁰

4. ANALYSE SECTORIELLE DE LA GOUVERNANCE PUBLIQUE

86. Cette partie examine l'impact des systèmes d'IA dans des domaines clés de la gouvernance publique, en se concentrant sur leurs implications pour les droits humains. S'appuyant sur la CEDH et la CSE, ainsi que sur d'autres instruments internationaux le cas échéant, il explore les secteurs où l'intégration des systèmes d'IA peut porter gravement atteinte aux droits humains et où une telle intégration est avancée ou

¹⁵⁸ Le Conseil de l'Europe applique la méthodologie HUDERIA dans ses activités de renforcement des capacités, telles que l'Académie HUDERIA, qui propose des sessions de formation aux fonctionnaires, aux régulateurs sectoriels, aux institutions publiques, aux professionnels du secteur, aux représentants du monde universitaire et de la société civile. HUDERIA sert également de base à la collaboration avec les développeurs d'IA du secteur privé sur des questions liées à la mise en œuvre de la Convention-cadre.

¹⁵⁹ CM/Rec(2016)3, paragraphe 20.

¹⁶⁰ Idem.

raisonnablement envisageable. Les descriptions sectorielles au début de chaque secteur ne sont pas exhaustives et peuvent inclure d'autres activités, en fonction des contextes nationaux ou des développements futurs.

87. Dans tous ces secteurs, la méthodologie HUDERIA du Conseil de l'Europe peut être utilisée comme cadre pour l'identification, l'évaluation, la prévention, l'atténuation et la gouvernance réglementaire plus large des risques liés à l'IA pour les droits de l'homme, la démocratie et l'État de droit.

4.1. Administration de la justice

88. L'administration de la justice englobe les systèmes, les processus et les institutions chargés de faire respecter la loi, de résoudre les litiges et de garantir l'équité et la justice. Elle comprend les tribunaux, les juges, les procureurs et les avocats, ainsi que les organismes chargés de l'application de la loi.

Principaux cas d'utilisation de l'IA

89. Au moment de la rédaction du présent document, 160 systèmes intégrés d'IA ont été jusqu'ici documentés comme étant utilisés ou pilotés au sein de systèmes judiciaires à travers l'Europe et dans d'autres pays participant au Réseau européen de cyberjustice du Conseil de l'Europe¹⁶¹. Les systèmes d'IA pourraient offrir de nouvelles possibilités et une chance d'améliorer la protection des droits humains et le respect du droit à être entendu dans un délai raisonnable s'ils sont développés et utilisés de manière appropriée, par exemple dans la mesure où les normes et la jurisprudence de la CEDH sont intégrées dans les outils de recherche et d'analyse ou d'aide à la décision facilités par l'IA. Si les systèmes d'IA conçus pour des tâches administratives auxiliaires présentent un risque minime¹⁶², ceux qui aident directement les autorités judiciaires à rechercher, interpréter les faits et appliquer la loi à des cas spécifiques présentent des risques importants pour le droit à un procès équitable et les droits humains connexes. L'administration de la justice a été l'un des premiers secteurs de la gouvernance publique dans lesquels le Conseil de l'Europe a abordé les implications de l'utilisation des systèmes d'IA sur

¹⁶¹ Le Centre de ressources sur la cyberjustice et l'IA sert de point de contact accessible au public pour obtenir des informations fiables sur les systèmes d'IA et autres outils de cyberjustice, dans le but de fournir un point de départ pour un examen plus approfondi de leurs risques et avantages pour les professionnels et les utilisateurs finaux. Il est supervisé par le Comité d'experts sur l'intelligence artificielle de la CEPEJ (<https://www.coe.int/en/web/cepej/ai-advisory-board>).

¹⁶² Comme l'anonymisation ou la pseudonymisation de décisions judiciaires, de documents ou de données, la communication entre le personnel et l'automatisation d'autres tâches administratives.

les droits en publiant sa « [Charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires et leur environnement](#) » (la « Charte éthique »)¹⁶³.

90. Les principaux cas d'utilisation de l'IA dans ce contexte sont les suivants :

- **Recherche, examen, analyse et découverte à grande échelle facilités par l'IA** : des systèmes d'IA qui créent une collection consultable de descriptions de jurisprudence, de textes juridiques et d'autres informations à partager avec des experts juridiques pour une analyse plus approfondie et une découverte à grande échelle sur des volumes importants de documents électroniques. Il s'agit par exemple de moteurs de recherche avec des interfaces appliquées à la jurisprudence et aux dossiers judiciaires.
- **Aide à la décision** : des systèmes qui facilitent ou automatisent les étapes du processus décisionnel. Il s'agit par exemple de résumer des textes, d'extraire des informations spécifiques dans une application, de fournir des lignes directrices et des points de repère et de calculer des barèmes pour les condamnations et les indemnisations. Jusqu'à présent, aucun processus décisionnel entièrement automatisé sans supervision humaine n'a été signalé en Europe.
- **Prédiction des résultats judiciaires** : des systèmes qui apprennent à partir de grands ensembles de données afin d'identifier des modèles dans les données qui sont ensuite utilisés pour visualiser, simuler ou prédire de nouvelles issues de litiges.
- **Règlement en ligne des litiges** ('*Online dispute resolution*' ou '*ODR*') : des technologies utilisées pour la résolution des litiges entre les parties avec une intervention humaine limitée. Il s'agit principalement de modes alternatifs de résolution des conflits, mais aussi de la résolution des conflits dans le cadre des tribunaux.
- **La nomination des juges et l'attribution des affaires basées sur l'IA** : Systèmes utilisés pour accomplir ou faciliter des tâches telles que l'attribution des affaires aux tribunaux et aux juges et l'établissement de niveaux de priorité.

¹⁶³ La Charte éthique, adoptée par la Commission européenne pour l'efficacité de la justice (CEPEJ) du Conseil de l'Europe, est l'un des premiers documents réglementaires sur l'IA qui fournit un ensemble de principes à mettre en œuvre par les acteurs publics et privés responsables de la conception et du développement d'outils et de services d'IA dans l'administration de la justice.

91. D'autres applications, telles que l'utilisation de l'IA pour l'interprétation pendant les audiences ou l'enregistrement, la transcription ou la traduction, pourraient également mettre en cause des éléments du droit à un procès équitable en fonction des circonstances.

Droits humains et principes pertinents

92. Les principes identifiés dans la Convention-cadre¹⁶⁴ et la Charte éthique européenne sur l'utilisation de l'intelligence artificielle correspondent à des préoccupations importantes et réelles concernant l'utilisation de l'IA dans l'administration de la justice et ses éventuelles répercussions négatives sur les droits humains protégés par la CEDH et la convention 108(+). Les principes de la Charte éthique européenne sur l'utilisation de l'intelligence artificielle comprennent le respect des droits fondamentaux, la non-discrimination, la qualité et la sécurité de l'IA, la transparence, l'impartialité et l'équité, ainsi que le principe du « contrôle par l'utilisateur »¹⁶⁵.

93. Le droit humain le plus touché dans ce secteur est le droit à un procès équitable, garanti par l'article 6 de la CEDH¹⁶⁶. Le droit à la liberté et à la sécurité, garanti par l'article 5 de la CEDH, est également en cause dans la mesure où il implique des règles spéciales en matière de protection judiciaire contre la privation arbitraire de liberté.

Le droit à un procès équitable

94. L'article 6 de la CEDH s'applique aux procédures impliquant la détermination des droits et obligations civils ou toute accusation pénale. Le principe clé régissant l'article 6 est l'équité¹⁶⁷. Comme l'a souligné la Cour, ce qui constitue un procès équitable ne peut faire l'objet d'une règle unique et constante, mais doit dépendre des circonstances de chaque affaire et à la lumière de l'équité globale de la procédure¹⁶⁸. Certains principes subsidiaires d'équité sont également particulièrement pertinents dans le contexte de l'IA :

¹⁶⁴ Convention-cadre (articles 4 à 13).

¹⁶⁵ Le principe du « contrôle par l'utilisateur » exclut toute approche normative et garantit que les utilisateurs sont des acteurs informés et maîtres de leurs choix.

¹⁶⁶ Ainsi que d'autres instruments internationaux relatifs aux droits humains (articles 10 et 11 de la Déclaration universelle des droits de l'homme, article 14 du Pacte international relatif aux droits civils et politiques, article 47 de la Charte des droits fondamentaux de l'Union européenne, article 8 de la Convention américaine relative aux droits de l'homme - Pacte de San José, article 7 de la Charte africaine des droits de l'homme et des peuples) et dans l'ordre juridique constitutionnel des pays démocratiques.

¹⁶⁷ *Vacher c. France*, n° 20368/92, 17 décembre 1996.

¹⁶⁸ *Ibrahim et autres c. Royaume-Uni [GC]*, n° 50541/08, n° 50571/08, n° 50573/08, n° 40351/09, 13 septembre 2016, paragraphe 250.

(i) Indépendance et impartialité

95. L'article 6 garantit un procès équitable et public devant un tribunal indépendant et impartial établi par la loi¹⁶⁹. Le tribunal doit être indépendant à la fois des autres branches du gouvernement, telles que l'exécutif et le législatif, et des parties impliquées dans l'affaire¹⁷⁰. Le tribunal doit également être impartial, c'est-à-dire subjectivement libre de tout préjugé ou parti pris personnel, et doit offrir des garanties suffisantes pour exclure tout doute légitime à cet égard¹⁷¹.

96. La partialité des systèmes d'IA peut ne pas être facilement discernable par le juge en raison de la perception généralisée de la « neutralité » algorithmique/mathématique et de la partialité technologique des juges eux-mêmes. Cela pourrait conduire à des résultats discriminatoires. Le recours intensif à l'IA pourrait conduire à une « standardisation » des décisions judiciaires, les juges se sentant obligés de suivre les recommandations de l'IA en raison de la « supériorité » perçue, en particulier dans les systèmes où leur mandat n'est pas permanent mais soumis à un vote populaire¹⁷², ou dans lesquels leur responsabilité personnelle (disciplinaire, civile ou même pénale) est susceptible d'être engagée¹⁷³.

(ii) Présomption d'innocence

97. Le principe de la présomption d'innocence dans les procédures pénales exige, entre autres, que : (i) les juges (et les jurés le cas échéant) doivent aborder leurs fonctions sans aucune idée préconçue de la culpabilité de l'accusé ; (ii) la charge de la preuve incombe à l'accusation, et (iii) tout doute doit profiter à l'accusé¹⁷⁴.

98. En raison du biais algorithmique, l'inclusion potentielle dans les systèmes d'IA de variables telles que les antécédents criminels et familiaux signifie que le sort d'une personne peut être affecté par le comportement passé d'un certain groupe sans qu'une attention appropriée soit accordée aux antécédents spécifiques de la personne

¹⁶⁹ Voir *Deweert c. Belgique*, n° 6903/75, 27 février 1980, paragraphe 49, Série A n° 35 ; *Kart c. Turquie* [GC], n° 8917/200, 3 décembre 2009, n° 8917/2005, paragraphe 67.

¹⁷⁰ *Beaumartin c. France*, n° 15287/89, 24 novembre 1994, paragraphe 38 ; *Sramek c. Autriche*, n° 8790/79, 22 octobre 1984, paragraphe 42.

¹⁷¹ *Findlay c. Royaume-Uni*, n° 22107/93, 25 février 1997, paragraphe 73 ; *Micallef c. Malte* [GC], n° 17056/06, 2009 paragraphe 93.

¹⁷² Parmi les États membres du Conseil de l'Europe, cela peut être le cas pour la nomination des juges cantonaux en Suisse.

¹⁷³ CEPEJ, *Charte éthique*, paragraphe 140.

¹⁷⁴ *Barberà, Messegue et Jabardo c. Espagne*, 6 décembre 1988, requête n° 10590/83, paragraphe 77.

accusée, à ses motivations et, en fin de compte, à sa culpabilité. Cela pourrait avoir pour conséquence d'interférer avec le droit d'une personne à être présumée innocente jusqu'à ce que sa culpabilité soit prouvée par un tribunal. Si l'utilisation d'outils prédictifs par les juges dans les procès pénaux est très rare en Europe¹⁷⁵, il existe dans d'autres juridictions des exemples concrets d'effets négatifs¹⁷⁶.

(iii) L'égalité des armes et procédure contradictoire

99. L'égalité des armes est une caractéristique inhérente à un procès équitable. Elle exige que chaque partie ait une possibilité raisonnable de présenter sa cause dans des conditions qui ne la placent pas dans une situation désavantageuse par rapport à son adversaire et s'applique aux procédures pénales et civiles¹⁷⁷. Dans un contexte pénal, le droit à une procédure contradictoire signifie que l'accusé a la possibilité de prendre connaissance et de commenter toutes les preuves produites ou observations déposées en vue d'influencer la décision du tribunal, leur existence, leur contenu et leur authenticité sous une forme et dans un délai approprié¹⁷⁸. Le fait de ne pas communiquer à la défense des éléments de preuve matériels susceptibles de permettre à l'accusé de se disculper ou d'obtenir une réduction de sa peine constituerait un refus des moyens nécessaires à la préparation de la défense, et constituerait donc une violation de l'Article 6.¹⁷⁹ Le droit à un procès contradictoire ne peut être ignoré dans le but de gagner du temps ou d'accélérer la procédure¹⁸⁰.

100. Dans le contexte de l'utilisation des systèmes d'IA, l'égalité des armes implique que, dans chaque cas, la partie doit être consciente du rôle du système dans la procédure, des critères de son fonctionnement et de son impact éventuel sur l'issue de l'affaire. Des problèmes peuvent se poser si une partie se voit refuser un accès suffisant pour examiner les données analysées par l'IA et utilisées comme éléments de preuve¹⁸¹. Le

¹⁷⁵ Charte éthique, paragraphe 124.

¹⁷⁶ Idem, paragraphes 128-131.

¹⁷⁷ *Öcalan c. Turquie* [GC], n° 46221/99, 12 mai 2005, paragraphe 140 ; *Foucher c. France*, n° 22209/93, 18 mars 1997, paragraphe 34 ; *Bulut c. Autriche*, n° 17358/90, 22 février 1996 ; *Faig Mammadov c. Azerbaïdjan*, n° 60802/09, 26 janvier 2017, paragraphe 19.

¹⁷⁸ *Rowe et Davis c. Royaume-Uni* [GC], n° 28901/95, 16 février 2000, paragraphe 60 ; *Kress c. France* [GC], n° 39594/98, 7 juin 2001, paragraphe 74 ; *Krčmář et autres c. République tchèque*, n° 35376/97, 3 mars 2000, paragraphe 42.

¹⁷⁹ *Natunen c. Finlande*, n° 21022/04, 31 mars 2009, n° 21022/04, paragraphe 43.

¹⁸⁰ *Nideröst-Huber c. Suisse*, n° 18990/91, 18 février 1997, paragraphe 30.

¹⁸¹ Voir *Sigurður Einarsson et autres c. Islande*, n° 39757/15, 4 septembre 2019. Dans cette affaire, les requérants se plaignaient de ne pas avoir accès à l'ensemble des données traitées par un système d'e-Discovery utilisé par l'accusation. La Cour a reconnu que le refus d'accès concernant au moins l'un des ensembles de preuves soulevait une question au regard de l'article 6 paragraphe 3 b) (paragraphe 91), mais

droit à une procédure contradictoire exigera probablement la possibilité de contester la validité scientifique, les préjugés et les erreurs potentielles d'un système d'IA. Cependant, les droits de propriété intellectuelle et les lois sur les secrets commerciaux peuvent restreindre l'accès aux systèmes d'IA privés utilisés par les autorités chargées de l'application de la loi. Même sans ces obstacles, la complexité des modèles utilisés (« le problème de la boîte noire » peut constituer un défi majeur pour le défendeur. En outre, si les systèmes d'IA peuvent accélérer les procédures en permettant de gagner du temps, le droit à une procédure contradictoire ne peut être négligé à cette fin.

101. Dans les procédures civiles, l'égalité des armes pourrait être compromise par un éventuel déséquilibre entre les parties au litige dans leur compréhension et leur capacité à utiliser les outils d'IA, en fonction de leurs moyens disponibles, y compris financiers, ou même de leur niveau de culture numérique. Dans ce contexte, la Recommandation CM/Rec(2016)3 du Comité des Ministres aux États membres sur les droits de l'homme et les entreprises souligne que lorsque des victimes présumées de violations des droits humains liées aux entreprises intentent des actions civiles contre des entreprises pour de telles violations, les États membres devraient veiller à ce que leurs systèmes juridiques garantissent suffisamment l'égalité des armes au sens de l'article 6 de la CEDH. En particulier, ils devraient prévoir dans leurs systèmes juridiques des régimes d'aide juridique pour les plaintes concernant de telles violations. Cette aide juridique devrait pouvoir être obtenue de manière pratique et efficace.¹⁸² Dans ce contexte, les outils d'IA pourraient également être développés pour fournir des informations juridiques et de l'assistance, et pourraient faciliter la recherche de protection des droits humains par les utilisateurs. Cependant, des mesures de sécurité appropriées devraient être mises en place lors de la conception de tels dispositifs.

(iv) Accès aux tribunaux

102. Le droit d'accès à un tribunal est un aspect inhérent aux garanties consacrées par l'article 6, et n'est pas plus absolu en matière pénale qu'en matière civile. Toute personne a le droit de porter devant une cour ou un tribunal toute réclamation relative à ses « droits et obligations de caractère

a conclu à la non-violation en raison du fait que l'accusation n'avait pas non plus connaissance du contenu de la collection complète de données et que les requérants n'avaient à aucun moment formellement demandé une ordonnance judiciaire pour accéder à la collection complète de données (paragraphe 89-93). Voir également l'opinion partiellement dissidente du juge Pavli, qui se concentre sur les questions relatives à l'utilisation des systèmes d'intelligence artificielle.

¹⁸² CM/Rec(2016)3, paragraphe 41.

civil »¹⁸³. Un individu doit avoir une possibilité claire et pratique de contester un acte qui constitue une ingérence dans ses droits¹⁸⁴. La nature pratique et effective de ce droit peut être altérée, par exemple, par une interprétation excessivement formaliste des règles de procédure.

103. Dans ce contexte, le recours à des systèmes d'IA ne devrait pas entraver le droit d'accès à un tribunal au sens de l'article 6¹⁸⁵ ; le contrôle humain sur la prise de décision devrait être assuré¹⁸⁶. L'accès au tribunal ne devrait pas non plus être entravé par des obstacles techniques liés à un système d'IA spécifique. À cet égard, en ne tenant pas compte des obstacles pratiques liés à l'utilisation obligatoire d'un système de dépôt électronique et en n'autorisant pas le dépôt alternatif (sur papier), une juridiction nationale peut adopter une approche excessivement formaliste qui équivaut à une violation de l'article 6 paragraphe 1¹⁸⁷.

Droit à la liberté et à la sûreté

104. Le principal objectif de l'article 5 est d'empêcher les privations de liberté illégales, arbitraires ou injustifiées¹⁸⁸. Pour satisfaire à l'exigence de légalité, la privation de liberté doit être conforme à une procédure prévue par la loi et soumise à un contrôle de sa légalité par un tribunal. Si les défauts d'un ordre de détention ne rendent pas automatiquement la détention illégale¹⁸⁹, le raisonnement qui sous-tend la décision ordonnant la détention d'une personne est un facteur pertinent pour déterminer si la

¹⁸³ *Golder c. Royaume-Uni*, n° 4451/70, 21 février 1975, paragraphe 36.

¹⁸⁴ *Bellet c. France*, n° 23805/94, 4 décembre 1995, paragraphe 38.

¹⁸⁵ Voir la Résolution 2081 (2015) de l'Assemblée parlementaire du Conseil de l'Europe, « Accès à la justice et Internet : potentiel et défis », dans laquelle l'APCE a appelé à garantir que « les parties qui s'engagent dans des procédures ODR conservent le droit d'accéder à une procédure d'appel judiciaire satisfaisant aux exigences d'un procès équitable conformément à l'article 6 de la Convention ». Voir aussi les *Lignes directrices de la CEPEJ sur les modes alternatifs de résolution en ligne des litiges* (2023).

¹⁸⁶ Le droit à la surveillance humaine est également énoncé à l'article 9, paragraphe 1, point a), de la convention 108+.

¹⁸⁷ Voir *Xavier Lucas c. France*, 9 juin 2022, n° 15567/20, paragraphe 57, où la Cour a conclu à la violation de l'article 6 paragraphe 1 du fait que la Cour de cassation française n'avait pas pris en considération les obstacles pratiques, y compris les défauts techniques et matériels, d'une plateforme e-Barreau qui avait empêché le requérant de soumettre par voie électronique une demande d'ouverture d'une procédure. Voir également *Farcaș et autres c. Roumanie*, n° 30502/05, 5 juin 2018, où la Cour a estimé que le droit d'accès à la justice des requérants était devenu illusoire du fait que les documents judiciaires avaient été signifiés uniquement par publication (sur papier et en ligne) dans le Bulletin des procédures d'insolvabilité, alors que les requérants n'avaient ni les ressources financières pour consulter la version papier ni l'accès à Internet pour consulter la version électronique.

¹⁸⁸ *Selahattin Demirtaş c. Turquie* (n° 2) [GC], n° 14305/17, 22 décembre 2020, paragraphe 311.

¹⁸⁹ *Ječius c. Lituanie*, 2000, n° 34578/97, 31 juillet 2000, paragraphe 68.

détention doit être considérée comme arbitraire au sens de l'article 5, paragraphe 1¹⁹⁰.

105. La privation de liberté est également illégale au sens de l'article 5 si elle résulte d'une condamnation prononcée à l'issue d'une procédure « manifestement contraire aux dispositions de l'article 6 ou aux principes qui y sont consacrés », au point de constituer un « déni de justice flagrant ».¹⁹¹ Un procès sommaire qui ne permet pas une évaluation approfondie et objective du cas d'une personne qui est ensuite condamnée à une peine d'emprisonnement pourrait donc constituer une violation non seulement de l'article 6, mais aussi de l'article 5 de la CEDH¹⁹².

106. Les questions soulevées au titre de l'article 6 (voir ci-dessus) s'appliquent également aux garanties judiciaires contre la détention arbitraire énoncées à l'article 5, paragraphes 3 et 4, qui prévoient respectivement que les détenus pénaux doivent être rapidement déférés devant un juge et que toute personne peut contester la légalité de sa détention devant un tribunal. Le manque de transparence ou de responsabilité des systèmes d'IA potentiels pourrait compromettre l'équité des décisions en matière de privation de liberté. Ils risquent de perpétuer les préjugés, ce qui pourrait conduire à des détentions provisoires injustes, à des condamnations disproportionnées ou à des refus injustes de libération conditionnelle. En outre, leur opacité compromet la capacité des individus à contester efficacement les décisions, ce qui soulève des questions quant à l'équité et à la responsabilité.

Vie privée et protection des données dans le cadre de l'administration de la justice

107. Les tribunaux et les autorités impliquées dans l'administration de la justice traitent et conservent des données à caractère personnel, y compris des données sensibles dont l'utilisation abusive pourrait entraîner des violations des données et de la vie privée ainsi que des discriminations¹⁹³. L'article 8 est violé lorsque des données sensibles sont conservées sans garanties adéquates. Un juste équilibre doit être

¹⁹⁰ *S., V. et A. c. Danemark* [GC], n° 35553/12, 36678/12 et 36711/12, 22 octobre 2018, paragraphe 92.

¹⁹¹ *Willcox et Hurford c. Royaume-Uni (déc.)*, Nos. 43759/10 et 43771/12, 8 janvier 2013, paragraphe 95 ; *Othman (Abu Qatada) c. Royaume-Uni*, n° 8139/2009, 17 janvier 2012, paragraphe 259 ; *Stoichkov c. Bulgarie*, n° 9808/02, 24 mars 2005, paragraphes 51, 56-58. Ce qui est requis, c'est une violation des principes d'un procès équitable si fondamentale qu'elle équivaut à une annulation ou à une destruction de l'essence même du droit garanti par l'article 6 (*Othman*, paragraphe 260).

¹⁹² Voir *Vorontsov et autres c. Ukraine*, 2021, paragraphes 42-49.

¹⁹³ Convention 108(+), article 6.

maintenu entre la nécessité de rendre publiques les décisions judiciaires et le respect des droits fondamentaux des parties ou des témoins¹⁹⁴.

108. Les outils d'anonymisation ou de pseudonymisation intégrant la technologie de l'IA, tels que ceux déjà en place dans plusieurs États membres du Conseil de l'Europe, peuvent s'avérer utiles pour dissimuler systématiquement toute information permettant d'identifier les individus. Toutefois, Les préoccupations générales concernant le risque que représentent les systèmes d'IA pour la vie privée et la protection des données continuent de s'appliquer à mesure que ces outils sont développés. La meilleure approche pour renforcer la confidentialité consiste à « réduire au minimum ou éliminer la nécessité pour une organisation de former un modèle d'IA à la collecte de données personnelles ». ¹⁹⁵

Pour en savoir plus

- Résolution 2081 de l'Assemblée parlementaire du Conseil de l'Europe, [Accès à la justice et Internet : potentiel et défis](#), 2015
- Résolution 2342 de l'Assemblée parlementaire du Conseil de l'Europe, [Justice par algorithme – Le rôle de l'intelligence artificielle dans les systèmes de police et de justice pénale](#), 2020
- Commission européenne pour l'efficacité de la justice (CEPEJ), [Charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires et leur environnement](#), 2018
- Commission européenne pour l'efficacité de la justice (CEPEJ), [Glossaire Cyberjustice et IA](#)
- Commission européenne pour l'efficacité de la justice (CEPEJ), [Lignes directrices sur la numérisation des dossiers judiciaires et la digitalisation des tribunaux](#), 2021
- Commission européenne pour l'efficacité de la justice (CEPEJ), [Lignes directrices sur les modes alternatifs de règlement en ligne des litiges](#), 2023, y compris les bonnes pratiques liées aux lignes directrices.
- Commission européenne pour l'efficacité de la justice (CEPEJ), [Note d'information sur l'utilisation de l'IA générative par les professionnels de la justice dans un contexte professionnel](#), 2024
- Comité européen de coopération juridique (CDPC), [Intelligence artificielle et droit administratif, étude comparative](#), 2022, en anglais uniquement ; Conseil de l'Europe, [Centre de ressources](#)

¹⁹⁴ Sauf dans les cas où la nécessité de protéger la confidentialité de certains types de données à caractère personnel est contrebalancée par l'intérêt de la recherche et de la poursuite d'infractions et de la publicité des procédures judiciaires. *Avilkina et autres c. Russie*, 2013, paragraphe 45 ; *Z c. Finlande*, 1997, paragraphe 97.

¹⁹⁵ Sharing trustworthy AI models with privacy-enhancing technologies, *OECD Artificial Intelligence Papers*, n° 38, 2025 (en anglais uniquement, traduction libre).

sur la cyberjustice et l'IA. Des informations détaillées sur le déploiement et l'utilisation des outils numériques dans l'administration de la justice sont disponibles dans les [profils nationaux](#) individuels.

- Conseil consultatif des juges européens (CCJE) du Conseil de l'Europe, [Moving Forward: the use of assistive technology in the judiciary](#), Opinion n° 26, 2023, en anglais uniquement.
- Concernant les systèmes d'IA destinés au secteur privé : Liquid Legal Institute (LLI), [First Global Report on the State of Artificial Intelligence in Legal Practice](#), 2023, en anglais uniquement.
- OCDE, [Governing with Artificial Intelligence: The State of Play and Way Forward in Core Government Functions](#), 2025, en anglais uniquement.
- Initiative mondiale des juges de l'UNESCO, une enquête sur l'utilisation des systèmes d'IA par les opérateurs judiciaires : [UNESCO Global Judges' Initiative: survey on the use of AI systems by judicial operators](#), 2024, en anglais uniquement.
- Ministère de la Justice de l'Espagne, [Policy on the Use of Artificial Intelligence in the Administration of Justice](#), 2024, en anglais uniquement.
- Magistrats des cours et tribunaux du Royaume-Uni, [Artificial Intelligence \(AI\), Guidance for Judicial Office Holders](#), 2025, en anglais uniquement.

4.2. Application de la loi et la sécurité publique

109. Ce secteur comprend la police¹⁹⁶, les services de renseignement et assimilés¹⁹⁷, y compris des questions telles que l'identification des personnes à des fins d'application de la loi, la prévention de la criminalité, les enquêtes criminelles, les programmes concernant la protection des personnes en danger (par exemple, les victimes de violence domestique ou les témoins protégés), les arrestations et les détentions, la prison et la probation la gestion des foules lors d'événements publics et le maintien de l'ordre public, la lutte contre le terrorisme, les opérations de sécurité nationale, les mesures impliquant la surveillance des communications, les restrictions, les interdictions, les fermetures, les diverses formes de surveillance, y compris celles qui affectent la liberté de mouvement.

¹⁹⁶ Dans le contexte de ce Manuel, la « police » désigne les forces ou services de police traditionnels et d'autres services autorisés et/ou contrôlés par l'État, chargés par ce dernier, dans le plein respect de l'État de droit, de fournir des services de maintien de l'ordre.

¹⁹⁷ Départements ou unités du gouvernement qui sont considérés comme équivalents aux services de renseignement du point de vue de leur fonction.

Principaux cas d'utilisation de l'IA¹⁹⁸

- **La criminalistique numérique** : Plusieurs outils et techniques de récupération et d'analyse des données ont été développés avec des composants d'IA. Ces outils permettent de récupérer des fichiers effacés, d'accéder à des données provenant d'appareils endommagés, de restituer des éléments d'information fragmentés dans des formats cohérents et d'étudier l'empreinte numérique des criminels.
- **Systèmes de surveillance** : technologies telles que la classification d'images, la vision par ordinateur et la biométrie, y compris la reconnaissance faciale et vocale automatisée, ou les empreintes digitales.
- **Analyse de données** utilisant des méthodes statistiques pour extraire des informations de vastes ensembles de données, par exemple sur les casiers judiciaires, les événements et les facteurs environnementaux identifiés dans les études criminologiques, ainsi que des données non structurées provenant de sources de renseignements en libre accès et des réseaux sociaux.
- **Traitement du langage naturel** : exécution de tâches par le traitement de données textuelles, telles que la classification et le regroupement de textes, le résumé de textes et la traduction automatique, par exemple la transcription de déclarations de témoins, l'analyse de documents juridiques ou l'extraction d'informations clés à partir de dossiers judiciaires.

Droits humains et principes pertinents

110. Le développement et l'utilisation de systèmes d'IA dans le domaine de l'application de la loi et de la sécurité publique pourrait présenter des risques particuliers pour les droits humains. En effet, les décisions qui pourraient être prises sur la base des résultats des systèmes d'IA, telles que la surveillance, les perquisitions et les saisies, ou les arrestations et les détentions, ont un fort impact sur les droits humains. L'utilisation de systèmes d'IA dans ce secteur peut interférer avec les articles 5 (droit à la liberté et à la sécurité), 8 (droit au respect de la vie privée et familiale), 10 (liberté d'expression) et 11 (liberté de réunion et d'association) de la CEDH, ainsi que l'article 2 du protocole n° 4 à la CEDH (liberté de circulation).¹⁹⁹ Les États peuvent justifier l'ingérence dans les articles 8, 10 et 11 de la CEDH par les buts légitimes énumérés dans le texte de ces articles, notamment la sécurité nationale, la sûreté publique ou la défense de l'ordre et la prévention des infractions pénales.

¹⁹⁸ Basé sur le rapport suivant : Europol : AI and policing - The benefits and challenges of artificial intelligence for law enforcement (2024) (*en anglais uniquement*).

¹⁹⁹ Applicable aux États qui ont ratifié le présent Protocole.

Le droit à la liberté et à la sécurité

111. Les systèmes de police prédictive font des estimations et des prédictions qui peuvent être transformées en actions ou décisions concrètes par le système de justice pénale, y compris en matière d'arrestation et de détention. En raison des décisions qui pourraient être prises sur la base des résultats de ces systèmes, des questions relatives à l'article 5 de la CEDH (droit à la liberté et à la sûreté) peuvent se poser. Les décisions d'arrestation ou de détention doivent être fondées sur des soupçons raisonnables, vérifiables et objectifs directement liés à une activité criminelle.²⁰⁰ Si les informations fournies par les systèmes de police prédictive sont utilisées pour corroborer les soupçons raisonnables justifiant une décision d'arrestation ou de détention, les questions d'explicabilité et d'interprétabilité (le « problème de la boîte noire ») concernant les systèmes d'IA peuvent poser des difficultés pour satisfaire aux critères requis de vérifiabilité et d'objectivité. Les méthodes de police prédictive ne doivent pas conduire à des décisions illégales de privation de liberté. Ces opérations menées par les autorités publiques doivent donc être légales, nécessaires et proportionnées aux objectifs poursuivis et se fonder sur un droit interne clair, prévisible et accessible, poursuivant un but légitime tout en assurant des garanties adéquates.²⁰¹

Vie privée et protection des données ; liberté d'expression et liberté de réunion et d'association

112. L'utilisation de systèmes d'IA dans le cadre de l'application de la loi peut avoir une incidence sur les articles 8 (droit au respect de la vie privée et familiale), 10 (liberté d'expression) et 11 (liberté de réunion et d'association) de la CEDH, ainsi que l'article 2 du protocole n° 4 à la CEDH (liberté de circulation). La jurisprudence de la Cour met en évidence les risques que présente l'utilisation généralisée des systèmes d'IA dans ce secteur pour la pleine jouissance de ces droits.

113. Le stockage ou la divulgation de données relatives à la vie privée d'une personne par une autorité chargée de l'application de la loi ou un service de sécurité constitue une ingérence dans le droit prévu à l'article 8²⁰² et le besoin de garanties sera d'autant plus grand lorsqu'il s'agit de la protection des données à caractère personnel faisant l'objet d'un

²⁰⁰ *Akgün c. Turquie*, n° 19699/18, 20 juillet 2021, paragraphes 156 et 175.

²⁰¹ Voir également l'article 5, point d), de la loi européenne sur l'IA, qui concerne l'utilisation des systèmes d'IA dans le domaine de l'application de la loi.

²⁰² *Leander c. Suède*, n° 9248/81, 26 mars 1987, paragraphe 48.

traitement automatisé, en particulier lorsque ces données sont utilisées à des fins répressives²⁰³.

114. La Convention 108(+) autorise également des exceptions aux dispositions relatives à la protection des données à caractère personnel pour des raisons de sécurité nationale, de sûreté publique et d'enquête sur des infractions pénales ; elle exige toutefois des États parties qu'ils mettent en place des garanties et des limitations pour s'assurer que toute exception reste nécessaire et proportionnée²⁰⁴. En outre, les activités de traitement à des fins de sécurité nationale doivent faire l'objet d'un examen et d'un contrôle indépendants et efficaces dans le cadre de la législation nationale de la partie concernée²⁰⁵.

Interception des communications et surveillance secrète

115. Les technologies de surveillance basées sur l'intelligence artificielle, notamment la reconnaissance faciale et l'identification biométrique à distance, posent de nouveaux défis en matière de protection des droits de l'homme. Ces technologies améliorent considérablement la portée, la rapidité et l'ampleur de la surveillance, y compris les interceptions massives, augmentant ainsi les risques, par exemple, de collecte massive de données, de violations graves de la vie privée ou de profilage. Parallèlement, les systèmes d'intelligence artificielle peuvent être opaques, biaisés ou sujets à des erreurs.

116. La surveillance d'un individu par les forces de l'ordre ou les services de sécurité implique généralement une ingérence dans la vie privée, protégée par l'article 8 de la CEDH²⁰⁶. Les pouvoirs de surveillance secrète des citoyens ne sont autorisés par la CEDH que dans la mesure où ils sont strictement nécessaires à la sauvegarde des institutions démocratiques²⁰⁷. La surveillance doit être motivée par des raisons pertinentes et suffisantes et être proportionnées au but légitime poursuivi²⁰⁸. La surveillance secrète doit être exercée conformément à la loi. En général, cela implique que la mesure contestée doit avoir un fondement dans le droit interne, lequel doit être suffisamment accessible et formulé avec une précision suffisante pour permettre à ceux à qui il s'applique de régler leur conduite et, si nécessaire, avec des conseils

²⁰³ *S. et Marper, c. Royaume-Uni* [GC], n^{os} 30562/04 et 30566/04, 4 décembre 2008, paragraphe 103.

²⁰⁴ Article 11, paragraphe 1, point a), et paragraphe 3.

²⁰⁵ Ibid.

²⁰⁶ *Amann c. Suisse* [GC], n^o 27798/95, paragraphes 69-70, CEDH 2000-II ; *Kopp c. Suisse*, n^o 23224/94, 25 mars 1998, paragraphe 53.

²⁰⁷ *Rotaru c. Roumanie* [GC], n^o 28341/95, 4 mai 2000, paragraphe 47 ; Szabó et Vissy c. Hongrie, n^o 37138/14, 12 janvier 2016, paragraphe 54 avec d'autres références.

²⁰⁸ *Segerstedt-Wiberg et autres c. Suède*, n^o 62332/00, 6 juin 2006, paragraphe 88.

appropriés, de prévoir, dans une mesure raisonnable compte tenu des circonstances, les conséquences que peut entraîner une action donnée²⁰⁹. Dans le contexte particulier des mesures de surveillance secrètes, telles que l'interception de communications, la « prévisibilité » signifie que le droit interne doit être suffisamment clair pour donner aux citoyens une indication adéquate des circonstances et des conditions dans lesquelles les autorités publiques sont habilitées à recourir à de telles mesures²¹⁰.

117. Les mesures de surveillance secrète doivent également être « nécessaires dans une société démocratique » pour atteindre un objectif légitime. Les autorités nationales disposent d'une large marge d'appréciation pour choisir la meilleure manière d'atteindre les objectifs légitimes, notamment celui de protéger la sécurité nationale²¹¹. Toutefois, « compte tenu du risque qu'un système de surveillance secrète destiné à protéger la sécurité nationale puisse, sous couvert de la défendre, porter atteinte à la démocratie, voire la détruire », des garanties adéquates et efficaces contre les abus sont nécessaires²¹². Des facteurs tels que « la nature, la portée et la durée des mesures envisageables, les motifs requis pour les ordonner, les autorités compétentes pour les autoriser, les mettre en œuvre et les contrôler, ainsi que le type de recours prévu par le droit national » sont pertinents pour déterminer la conformité avec la CEDH²¹³.

²⁰⁹ *Vavříčka et autres c. République tchèque* [GC], n^{os} 47621/13 et 5 autres, 8 avril 2021, paragraphe 266 avec d'autres références. Voir également *Plechlo c. Slovaquie*, n^o 25132/13, 18 avril 2017, paragraphe 43 ; voir également *Big Brother Watch et autres c. Royaume-Uni* [GC], n^{os} 58170/13, 62322/14 et 24960/15, 25 mai 2021, paragraphe 332 ; *Roman Zakharov c. Russie* [GC], n^o 47143/06, 4 décembre 2015, paragraphe 228 ; voir également, parmi de nombreuses autres autorités, *Rotaru c. Roumanie* [GC], n^o 28341/95, paragraphe 52, CEDH 2000-V ; *S. et Marper c. Royaume-Uni* [GC], n^{os} 30562/04 et 30566/04, 4 décembre 2008, paragraphe 95 ; *Kennedy c. Royaume-Uni*, n^o 26839/05, 18 mai 2010, paragraphe 151.

²¹⁰ *Big Brother Watch et autres c. Royaume-Uni* [GC], n^{os} 58170/13, 62322/14 et 24960/15, 25 mai 2021, paragraphe 333 ; *Leander c. Suède*, n^o 9248/81, 26 mars 1987, paragraphe 51.

²¹¹ *Ibid* ; *Škoberne c. Slovénie*, n^o 1310/10, 12 décembre 2017, paragraphe 124.

²¹² *Plechlo c. Slovaquie*, n^o 25132/13, 18 avril 2017, paragraphe 43 (*traduction libre ; en anglais uniquement*).

²¹³ *Škoberne c. Slovénie*, n^o 1310/10, 12 décembre 2017, paragraphe 124 ; voir également *Roman Zakharov c. Russie* [GC], n^o 47143/06, 4 décembre 2015, paragraphe 232 ; *İrfan Güzel c. Turquie*, n^o 35285/08, 7 février 2017, paragraphe 85 ; *Ekimdzhiiev et autres c. Bulgarie*, n^o 70078/12, 11 janvier 2022, paragraphes 418-419 ; voir également *Big Brother Watch et autres c. Royaume-Uni* [GC], n^{os} 58170/13, 62322/14 et 24960/15, 25 mai 2021 ; *Centrum för rättvisa c. Suède* [GC], n^o 35252/08, 25 mai 2021 ; *Podchasov c. Russie*, n^o 33618/19, 2024, paragraphe 64.

118. Six garanties minimales sont requises pour éviter les abus lorsque des communications sont interceptées dans le cadre d'enquêtes pénales : la nature de l'infraction justifiant l'interception, les catégories de personnes concernées, les délais, les procédures de traitement des données, les garanties pour le partage des données et les conditions d'effacement²¹⁴. Dans un domaine où les abus dans des cas individuels sont potentiellement si faciles et peuvent avoir des conséquences si néfastes pour la société démocratique dans son ensemble, il est en principe souhaitable de confier le contrôle de surveillance à un juge²¹⁵, bien que la surveillance par des organismes non judiciaires puisse également être considérée comme conforme à la CEDH si l'organisme de surveillance est indépendant des autorités qui effectuent la surveillance et est doté de pouvoirs suffisants pour exercer un contrôle efficace et continu²¹⁶. En outre, lorsqu'un juge ou un tribunal chargé du contrôle adopte une attitude passive et se contente d'approuver, sans véritablement vérifier les faits, ce contrôle n'est pas compatible avec l'article 8²¹⁷.

119. La surveillance fondée sur des systèmes d'IA devrait reposer sur une législation accessible et prévisible, poursuivre un objectif légitime et inclure un contrôle rigoureux, y compris une protection judiciaire le cas échéant, afin de protéger le droit au respect de la vie privée (article 8), la liberté d'expression (article 10) et la liberté de réunion et d'association (article 11).

120. Les technologies de surveillance basées sur l'IA, notamment la surveillance biométrique et le suivi comportemental, peuvent également être utilisées pour renforcer la sécurité dans les prisons. Le fait de placer une personne sous surveillance vidéo permanente pendant son séjour en prison – ce qui constitue déjà une restriction considérable de sa vie privée – doit être considéré comme une ingérence grave dans le droit au respect de la vie privée, tel que protégé par l'article 8 de la CEDH²¹⁸. La [recommandation CM/Rec\(2024\)5](#) concernant les aspects éthiques et organisationnels de l'utilisation de l'IA et des technologies numériques connexes par les services pénitentiaires et de probation souligne que l'utilisation de ces systèmes pour maintenir la sûreté, la sécurité et le bon ordre doit être strictement nécessaire, proportionnée à l'objectif poursuivi, éviter tout effet négatif sur la vie privée et le bien-être des délinquants et du personnel et ne causer en aucun cas un préjudice physique ou mental intentionnel ou une souffrance à une personne.

²¹⁴ *Big Brother Watch et autres*, paragraphe 335, avec d'autres références.

²¹⁵ *Big Brother Watch et autres*, paragraphe 336.

²¹⁶ *Roman Zakharov c. Russie* [GC], n° 47143/06, 4 décembre 2015, paragraphe 275.

²¹⁷ *Zoltán Varga et 2 autres c. Slovaquie*, n° 58361/12, 20 juillet 2021, paragraphes 155-163.

²¹⁸ *Vasilică Mocanu c. Roumanie*, n° 43545/13, 6 décembre 2016.

121. Des violations de l'article 8 relatives à la surveillance secrète ont été identifiées dans des affaires impliquant des militants des droits humains²¹⁹, des membres d'organisations non gouvernementales,²²⁰ des avocats,²²¹ des journalistes²²². En ce qui concerne les journalistes, les mesures de surveillance ciblée visant à découvrir leurs sources journalistiques peuvent également porter atteinte à leur droit à la liberté d'expression (article 10 de la CEDH), en l'absence de garanties adéquates dans la loi ou d'une exigence impérieuse d'intérêt public justifiant de telles mesures dans le cas concret.²²³ Le droit des journalistes de protéger leurs sources fait partie de la liberté de « recevoir et de communiquer des informations et des idées sans ingérence d'autorités publiques » protégée par l'article 10 et constitue l'une de ses garanties importantes²²⁴.

Reconnaissance faciale

122. La reconnaissance faciale consiste en le traitement automatique d'images numériques contenant les visages d'individus à des fins d'identification ou de vérification de ces individus à l'aide de modèles faciaux.²²⁵ Le problème en matière de protection de la vie privée est que les technologies de surveillance publique permettent de collecter de grandes quantités d'informations sur les citoyens, qui pourraient être utilisées à des fins diverses, non autorisées et illégales.²²⁶ Des mesures de sécurité minimales concernant la durée, le stockage, l'utilisation et la destruction des données personnelles (biométriques) collectées à l'aide de la technologie de reconnaissance faciale sont nécessaires pour garantir des garanties appropriées. L'utilisation de la technologie de reconnaissance faciale pour identifier les participants à des manifestations pacifiques peut constituer une violation du droit au respect de la vie privée (article 8) et de la liberté d'expression (article 10)²²⁷ ainsi que de la liberté de réunion (article 11). Les données à caractère personnel révélant les opinions politiques relèvent de la catégorie spéciale des données

²¹⁹ *Shimovolos c. Russie*, n° 30194/09, 21 juin 2011.

²²⁰ *Association « 21 décembre 1989 » et autres c. Roumanie*, n° 33810/07, 24 mai 2011.

²²¹ *Vasil Vasilev c. Bulgarie*, n° 7610/15, 16 novembre 2021.

²²² *Azer Ahmadov c. Azerbaïdjan*, n° 3409/10, 22 juillet 2021.

²²³ Voir la Recommandation CM/Rec(2016)4 du Comité des Ministres aux États membres sur la protection du journalisme et la sécurité des journalistes et autres acteurs des médias, paragraphes 7 et 38.

²²⁴ *Sanoma Uitgevers B.V. c. Pays-Bas [GC]*, n° 38224/03, 14 septembre 2010, paragraphe 50.

²²⁵ Comité consultatif de la Convention 108 (T-PD), Lignes directrices sur la reconnaissance faciale, p. 3.

²²⁶ OCDE (2025), *Gouverner avec l'intelligence artificielle : état des lieux et perspectives d'avenir dans les fonctions gouvernementales essentielles*, p. 262.

²²⁷ *Glukhin c. Russie*, n° 11519/20, 4 juillet 2023, paragraphe 85.

sensibles bénéficiant d'un niveau de protection accru.²²⁸ Dans le cadre de la mise en œuvre de la technologie de reconnaissance faciale, il est essentiel de disposer de règles détaillées régissant la portée et l'application des mesures, ainsi que de solides garanties contre le risque d'abus et d'arbitraire. Le besoin de garanties est d'autant plus grand lorsque la technologie de reconnaissance faciale est utilisée en direct²²⁹. Outre les préoccupations liées à l'article 8, l'utilisation d'une technologie de reconnaissance faciale très intrusive pour identifier et arrêter les participants à des actions de protestation pacifiques pourrait avoir un effet dissuasif²³⁰ sur les droits à la liberté d'expression (article 10 de la CEDH) et à la liberté de réunion (article 11 de la CEDH)²³¹.

123. Les technologies de reconnaissance faciale, en particulier les systèmes en temps réel, nécessitent des garanties renforcées contre les abus et les effets dissuasifs sur la liberté d'expression et de réunion. Les États membres devraient mettre en place des règles claires, un contrôle indépendant et des recours efficaces afin de prévenir les pratiques de surveillance arbitraires ou illégales qui risquent de porter atteinte aux droits humains et aux principes de dignité humaine et d'autonomie personnelle. [Les lignes directrices sur la reconnaissance faciale du Conseil de l'Europe](#)²³² fournissent des précisions supplémentaires sur les mesures que les gouvernements, les développeurs de reconnaissance faciale, les fabricants, les fournisseurs de services et les entités utilisant des technologies de reconnaissance faciale devraient suivre et appliquer pour s'assurer qu'elles ne portent pas atteinte aux droits humains.

Non-discrimination et égalité

124. L'application des systèmes d'IA au maintien de l'ordre et à la sécurité publique soulève également des inquiétudes quant aux biais algorithmiques pouvant conduire à des discriminations. Par exemple, plusieurs cas ont montré que les systèmes de reconnaissance faciale comportaient des biais, entraînant l'identification erronée de suspects et, dans certains cas, l'incarcération injustifiée de personnes innocentes²³³. De plus, les outils d'IA destinés à améliorer la technologie de

²²⁸ Ibid, paragraphes 76 et 86.

²²⁹ Ibid, paragraphe 82.

²³⁰ Bien que la Cour ne donne pas de définition de l'effet dissuasif, lorsqu'elle aborde cette question, elle fait référence aux mesures qui ont pour conséquence de dissuader les personnes physiques et morales d'exercer leurs droits par crainte d'être soumises à ces mesures, voir par exemple, *Wille c. Liechtenstein* [GC], n° 28396/95, 28 octobre 1999, paragraphe 50.

²³¹ *Glukhin c. Russie*, paragraphe 88.

²³² Adoptée par le Comité consultatif de la Convention 108 en 2021.

²³³ Étude CDADI/GEC (2023), pp. 22-23. D'autres exemples figurent dans la Résolution 2342 (2020) « Justice par algorithme - Le rôle de l'intelligence artificielle dans les systèmes de police et de justice pénale », paragraphe 7.

reconnaissance faciale, lorsqu'ils sont entraînés à partir de jeux de données inadéquats ou biaisés, peuvent réduire la précision de l'identification pour certains groupes.²³⁴ Les États devraient faire preuve de prudence en ce qui concerne l'identification, l'évaluation, la prévention et l'atténuation des risques de discrimination découlant de l'utilisation, par exemple, des technologies de reconnaissance faciale ou des systèmes d'identification biométrique à distance dans les secteurs du maintien de l'ordre et de la sécurité. Les États peuvent évaluer si de nouvelles réglementations sont nécessaires ou si des mesures spécifiques, y compris des interdictions explicites, doivent être mises en œuvre pour prévenir la discrimination²³⁵.

125. Dans le contexte des services pénitentiaires et de probation, la [Recommandation CM/Rec\(2024\)5](#) souligne que des garanties doivent être mises en place pour prévenir la discrimination, assurer l'équité procédurale et défendre la dignité humaine, afin que la gestion des prisons par l'IA reste compatible avec les droits fondamentaux et l'État de droit. Lors du développement de l'IA et des technologies numériques connexes en vue d'accroître la précision et l'objectivité de l'évaluation des risques, il convient de relever les défis des biais algorithmiques ainsi que de la qualité et de la représentativité des données. La conception et l'utilisation des outils d'évaluation des risques doivent tenir compte de la diversité sous toutes ses formes, y compris la perspective de genre, les différentes formes de handicap et le multiculturalisme, afin d'éviter toute discrimination. Lorsque ces outils sont utilisés pour personnaliser les plans de traitement et de réinsertion, il convient de veiller à éviter les préjugés. L'utilisation de ces outils ne devrait pas remplacer les contacts humains réguliers entre les professionnels et les délinquants, y compris, le cas échéant, le travail avec leurs familles et leurs enfants, conformément à la [Recommandation CM/Rec\(2018\)5 du Comité des ministres aux États membres concernant les enfants de détenus](#).

Droit à un recours effectif

126. L'application de systèmes d'intelligence artificielle [à l'application de la loi et à la sécurité publique](#) soulève des préoccupations quant au droit à un recours effectif (article 13).

²³⁴ OCDE (2025), *Governing with Artificial Intelligence: The State of Play and Way Forward in Core Government Functions*, p. 262, en anglaise uniquement

²³⁵ Voir également la loi européenne sur l'IA, préambule (33).

Pour en savoir plus

- [Recommandation CM/Rec\(2021\)8 du Comité des Ministres aux États membres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage](#)
- Rapport de la Commission des questions juridiques et des droits de l'homme de l'Assemblée parlementaire du Conseil de l'Europe (APCE), [La justice par algorithme - le rôle de l'intelligence artificielle dans les systèmes de police et de justice pénale](#), 2020, Doc. 15156
- CEDH, [Surveillance de masse](#), Fiche d'information
- CEDH, [Protection des données à caractère personnel](#), Fiche d'information
- CEDH, [Nouvelles technologies](#), Fiche d'information
- [Guide sur la jurisprudence dans le terrorisme](#)
- CEDH, [Sécurité nationale et jurisprudence européenne](#), Rapport préparé par la Division des recherches de la Cour, 2013
- Jim Murdoch & Ralph Roche, [The European Convention on Human Rights and Policing](#), 2015, en anglais uniquement
- Commission de Venise, [Report on a Rule of Law and Human Rights Compliant Regulation of Spyware](#), CDL-AD(2024)043, 2024, en anglais uniquement
- EUROPOL, [AI and policing: The benefits and challenges of artificial intelligence for law enforcement](#), 2023, en anglais uniquement
- Étude du Parlement européen, [Artificial Intelligence and Law Enforcement – Impact on Fundamental Rights](#), 2020, en anglais uniquement
- Conseil des droits de l'homme des Nations unies, [Résolution du Conseil des droits de l'homme des Nations unies sur la liberté d'opinion et d'expression](#), UN Doc A/HRC/RES/50/15, 8 juillet 2022
- Conseil des droits de l'homme des Nations unies, [Résolution du Conseil des droits de l'homme des Nations unies sur la promotion, la protection et la jouissance des droits de l'homme sur l'internet](#), UN Doc A/HRC/RES/47/16, 7 juillet 2021
- OCDE, [Governing with Artificial Intelligence: The State of Play and Way Forward in Core Government Functions](#), 2025

4.3. Immigration et contrôle des frontières

127. Ce secteur comprend les activités liées au contrôle des frontières, aux conditions et modalités d'entrée et de sortie du territoire de l'État, y compris la délivrance de visas ou d'autres types d'autorisations de voyage, les permis de séjour, l'expulsion et le renvoi, le statut de réfugié et d'asile

et les ajustements de statut, les services de traduction/interprétation, la production de transcriptions, la collecte et l'évaluation de preuves, dans le respect des obligations internationales en matière de droits de l'homme, y compris la protection contre le refoulement, la non-discrimination, la vie privée et les garanties procédurales.

Principaux cas d'utilisation de l'IA

128. L'IA est de plus en plus utilisée à tous les stades du contrôle de l'immigration et des frontières, avec un déploiement plus important dans les phases de pré-départ et d'arrivée. Son rôle dans la phase de retour reste limité en comparaison.

- **Systèmes d'identification et de vérification** : contrôles d'identité assistés par l'IA et utilisant la biométrie (par exemple, l'identification automatisée des empreintes digitales, le balayage de l'iris, et la reconnaissance faciale), y compris l'identification des demandeurs d'asile sans preuve documentaire de leur identité.
- **Analyse prédictive et systèmes d'évaluation des risques** : outils de prévision et d'alerte précoce dans le contexte du contrôle de l'immigration et des frontières.
- **Systèmes de surveillance alimentés par l'IA** : camps de réfugiés, installations d'hébergement de migrants et surveillance et contrôle des frontières à l'aide de caméras alimentées par l'IA, de la reconnaissance faciale et de drones alimentés par l'IA ; évaluations des risques assistées par l'IA.
- **Prise de décision et automatisation assistées par l'IA** : vérification et traitement des demandes d'asile assistés par l'IA (par exemple, reconnaissance faciale, vocale et dialectale, translittération des noms et analyse des données des téléphones portables) ; IA générative pour aider les agents chargés des dossiers à synthétiser et à analyser de grandes quantités de documents ; systèmes d'IA qui fournissent des informations sur les formalités d'immigration à accomplir et sur les conditions de vie et de travail auxquelles les demandeurs peuvent s'attendre dans le pays de destination.

Droits humains et principes pertinents

129. La CEDH ne garantit pas le droit d'entrer, de s'installer ou de résider dans un pays spécifique²³⁶, mais les États membres doivent exercer leur contrôle aux frontières dans le respect des obligations qui leur incombent en vertu de la CEDH. Les ressortissants étrangers se trouvant sur le territoire ou soumis à la juridiction extraterritoriale d'un État partie bénéficient de la protection de la CEDH. La jurisprudence impose également certaines limites au droit des États de refuser l'admission d'une personne à leurs frontières, par exemple lorsque cela équivaudrait à un *refoulement*.²³⁷

130. La CSE n'accorde pas non plus aux ressortissants étrangers un droit d'entrée ou de séjourner sur les territoires des autres parties. Le CSE (Révisée) a affirmé que les protections de la CSE peuvent être étendues aux ressortissants étrangers d'États non parties²³⁸, dans la mesure où les parties ont déjà garanti des droits identiques ou indissociables en vertu des traités relatifs aux droits humains, en particulier la CEDH. Toutefois, elle a noté que de telles obligations ne relèvent généralement pas de ses fonctions de contrôle. La CSE oblige les États parties à adopter des politiques d'immigration flexibles, à assouplir les réglementations en matière d'emploi²³⁹ et à faciliter le regroupement familial²⁴⁰.

131. Outre la CEDH et la CSE, le Conseil de l'Europe a adopté plusieurs autres instruments juridiques pertinents.²⁴¹

132. L'utilisation de systèmes d'IA dans le domaine de l'immigration et du contrôle des frontières peut soulever des questions importantes au regard de l'article 3 (interdiction de la torture), de l'article 8 (droit au respect de la vie privée et familiale), de l'article 14 (interdiction de discrimination) et de l'article 13 (droit à un recours effectif) ainsi que, le cas échéant, l'article 1 du protocole n°7 (garanties procédurales en cas d'expulsion d'étrangers) de la Convention européenne des droits de l'homme.

²³⁶ *Jeunesse c. Pays-Bas* [GC], n° 12738/10, 3 octobre 2014, paragraphe 103 ; *Maslov c. Autriche* [GC], n° 1638/03, paragraphe 68, CEDH 23 juin 2008 ; *Üner c. Pays-Bas* [GC], n° 46410/99, paragraphe 54, CEDH 2006-XII, 18 octobre 2000 ; *Boujlifa c. France*, n° 25404/94, 21 octobre 1997, paragraphe 42, Recueil 1997-VI ; *Abdulaziz, Cabales et Balkandali c. Royaume-Uni*, n° 9214/80, paragraphe 9473/8, CEDH 2006-XII. *France*, n° 25404/94, 21 octobre 1997, paragraphe 42, Recueil 1997-VI ; *Abdulaziz, Cabales et Balkandali c. Royaume-Uni*, n°s 9214/80, 9473/81 et 9474/81, 28 mai 1985, paragraphe 67.

²³⁷ *F.G. c. Suède* [GC], n° 43611/11, 23 mars 2016, paragraphe 117.

²³⁸ Conclusions 2004, Déclaration d'interprétation.

²³⁹ CSE, article 18 paragraphes 1-3.

²⁴⁰ CSE, article 19, paragraphe 6.

²⁴¹ Voir <https://www.coe.int/en/web/migration-and-refugees/council-of-europe-reference-documents-and-resources>1

Néanmoins, s'il est mis en œuvre de manière appropriée, il offre également des possibilités d'améliorer la protection des droits fondamentaux des personnes dans le besoin grâce à une gestion plus efficace des migrations et à un déroulement plus rapide des procédures.

Droit à la vie privée et à la protection des données

133. Les [principes généraux relatifs à la protection de la vie privée et des données](#) s'appliquent aux ressortissants étrangers qui se trouvent sous la juridiction de l'État.

134. L'utilisation de systèmes d'IA pour la gestion des frontières, tels que les drones équipés d'IA, les capteurs, la reconnaissance faciale et l'analyse prédictive utilisant des données à caractère personnel, doit reposer sur une base juridique et être proportionnée.²⁴² La protection de l'article 8 s'étend aux données à caractère personnel, y compris les données électroniques et les données biométriques²⁴³. La conservation généralisée et indiscriminée des données biométriques peut présenter un risque spécifique lié à l'utilisation de l'IA et, par conséquent, au droit au respect de la vie privée.²⁴⁴ Les données biométriques sont considérées comme des données sensibles²⁴⁵ et peuvent révéler des caractéristiques personnelles supplémentaires, telles que l'origine ethnique, l'état de santé ou le handicap. Par conséquent, une protection spéciale est nécessaire pour éviter toute utilisation abusive susceptible d'entraîner une discrimination. Les systèmes d'identification et de vérification basés sur les empreintes digitales, les scans de l'iris et la reconnaissance faciale présentent des risques, en particulier lorsque les données biométriques sont collectées, stockées, utilisées ou partagées sans garanties suffisantes.

135. Les systèmes d'IA peuvent générer des erreurs, en particulier lors du contrôle des données relatives aux voyageurs à des fins de sécurité, par exemple pour détecter des terroristes ou des criminels présumés. Ils peuvent également négliger des personnes en situation de vulnérabilité, telles que les victimes de la traite des êtres humains, les migrants sans

²⁴² Conseil des droits de l'homme des Nations Unies, Rapport « Impact de l'utilisation de services militaires et de sécurité privés dans la gestion de l'immigration et des frontières sur la protection des droits de tous les migrants » (2020) UN Doc A/HRC/45/9 ; AGNU, Rapport "Formes contemporaines de racisme, de discrimination raciale, de xénophobie et de l'intolérance qui y est associée" (2020) UN Doc A/75/590, en anglais uniquement ;

²⁴³ Voir *S. et Marper c. Royaume-Uni*, n^{os} 30562/04 et 30566/04, 4 décembre 2008, paragraphe 68 ; *Gaughran c. Royaume-Uni*, n^o 45245/15, 13 février 2020, paragraphe 68 ; *Brunet c. France*, requête n^o 21010/10, 18 septembre 2014, paragraphe 39.

²⁴⁴ *S. et Marper contre le Royaume-Uni*, n^{os} 30562/04 and 30566/04, 4 décembre 2008, paragraphe 125.

²⁴⁵ Convention 108+, article 8.

papiers ayant besoin de protection ou les personnes fuyant la persécution. Ces systèmes traitent souvent d'énormes ensembles de données provenant de multiples sources (police, services de renseignement, autorités frontalières et autorités compétentes en matière d'asile) et sont interopérables. Ces dernières ignorent souvent dans quelle mesure leurs données peuvent être incluses²⁴⁶. Dans de telles circonstances, la surveillance et la possibilité de contester une inclusion abusive et de demander une rectification pourraient être entravées. Selon les mesures spécifiques déclenchées par un signalement provenant d'une liste de surveillance (par exemple, interdiction de voyager, refus d'entrée ou de séjour, interrogatoire, surveillance ou même arrestation ou expulsion), cela peut avoir une incidence sur un large éventail de droits, notamment la liberté de circulation, le respect de la vie privée, le droit à la liberté et le droit à un procès équitable. Elle peut également avoir une incidence directe ou indirecte sur toute une série de droits civils, politiques, économiques, sociaux et culturels des membres de la famille, y compris les enfants, et des associés des personnes inscrites sur la liste. Afin d'éviter l'identification erronée de voyageurs comme suspects ou comme personnes représentant une menace liée au terrorisme, la pertinence des résultats individuels des évaluations automatiques devrait être soigneusement examinée par une personne de manière non automatisée²⁴⁷.

136. La création et la maintenance des systèmes d'IA utilisés à de telles fins, ainsi que la procédure régissant leur fonctionnement, doivent prévoir des garanties efficaces contre les abus²⁴⁸, notamment des délais de conservation des données et une protection particulière des données sensibles telles que les informations sur les opinions politiques d'une personne²⁴⁹, ainsi que la possibilité réelle de demander la suppression des données²⁵⁰ et la rectification des données erronées²⁵¹.

²⁴⁶ OSCE Policy Brief, Border Management and Human Rights, Collection, processing and sharing of personal data and the use of new technologies in the counter-terrorism and freedom of movement context (2021). p. 27 (*en anglais uniquement*).

²⁴⁷ Comité consultatif de la Convention 108 du Conseil de l'Europe, *Opinion on the Data protection implications of the processing of Passenger Name Records*, Strasbourg, 19 août 2016, p. 8 (*en anglais uniquement*).

²⁴⁸ *Shimovolos c. Russie*, n° 30194/09, 21 juin 2011, concernant l'enregistrement d'un militant des droits humains dans une « base de données de surveillance » qui suivait ses déplacements en train et en avion.

²⁴⁹ *Catt c. Royaume-Uni*, n° 43514/15, 24 janvier 2019, concernant la collecte et la conservation de données sur un militant de longue date dans une base de données de la police sur les « extrémistes nationaux ».

²⁵⁰ *Brunet c. France*, requête n° 21010/10, 18 septembre 2014.

²⁵¹ *Khelili c. Suisse*, n° 16188/07, 18 octobre 2011.

Non-discrimination

137. Les décisions fondées sur des informations provenant de systèmes d'IA peuvent donner lieu à une discrimination, y compris une discrimination indirecte et intersectionnelle, en raison des préjugés inhérents à ces systèmes. En outre, les technologies telles que les systèmes de reconnaissance faciale qui utilisent des données biométriques ont été décrites comme intrinsèquement faillibles, car elles reposent inévitablement sur des probabilités statistiques et sont sujettes à l'inexactitude et aux erreurs²⁵². Bien que cette question ne soit pas exclusivement liée à l'immigration, les conséquences pour les droits des migrants et des réfugiés peuvent être importantes. Si des systèmes d'IA basés sur des technologies de reconnaissance faciale sont utilisés pour l'identification et la vérification de l'identité avant le départ ou à l'arrivée aux frontières, certaines personnes peuvent être plus exposées à des inexactitudes et à des erreurs d'identification en raison de leurs caractéristiques protégées. Les outils de prise de décision assistée par ordinateur qui analysent le visage, la parole, la reconnaissance dialectale, la translittération du nom ou les données du téléphone portable dans les systèmes de visa et d'autorisation de voyage pourraient révéler par inadvertance des caractéristiques protégées, augmentant ainsi le risque d'évaluations biaisées et de traitement inégal, et leur utilisation abusive pourrait conduire à un profilage discriminatoire. Si ces préjugés et ces erreurs ne sont pas atténués, les personnes identifiées à tort ou victimes de discrimination pourraient se voir refuser l'entrée ou être renvoyées vers des pays où elles pourraient être exposées à des risques incompatibles avec la CEDH, y compris l'article 3.²⁵³

Droit à un recours effectif

138. La nature « boîte noire » des systèmes d'IA peut réduire la transparence et l'explicabilité, laissant les individus dans l'ignorance de la manière dont l'IA a influencé les décisions les concernant, telles que les refus de visa, les évaluations du statut de réfugié ou les ordonnances

²⁵² Les niveaux d'inexactitude des algorithmes de reconnaissance biométrique des visages dépendent fortement du sexe, de la couleur de la peau et de l'âge. Des études ont montré que les algorithmes de reconnaissance faciale existants avaient plus de difficultés à reconnaître les visages féminins et produisaient plus de faux rejets et de fausses acceptations pour les visages féminins. Ils produisaient des résultats plus précis pour les visages clairs que pour les visages foncés et avaient le taux d'erreur le plus élevé sur les visages féminins foncés. Voir *Border Management and Human Rights, Collection, processing and sharing of personal data and the use of new technologies in the counter-terrorism and freedom of movement context*, 5 octobre 2021 (*en anglais uniquement*).

²⁵³ Voir par exemple *Saadi c. Italie* [GC], n° 37201/06, 29 février 2008, paragraphe 125ff.

d'expulsion. Les biais liés à l'automatisation aggravent ces problèmes. Par exemple, l'existence d'une classification automatisée ou d'un score de risque peut affecter de manière significative les décisions des agents chargés des dossiers concernant les visas et les permis de séjour ou les demandes d'asile²⁵⁴.

139. Si les décisions relatives à l'immigration et aux questions connexes, telles que l'entrée, le séjour et l'éloignement des étrangers, ne relèvent pas du champ d'application de l'article 6 de la CEDH (droit à un procès équitable) car elles ne concernent pas les « droits et obligations de caractère civil »²⁵⁵, l'article 13 de la CEDH (droit à un recours effectif) est applicable lorsque d'autres droits substantiels de la CEDH sont en jeu. Par exemple, la jurisprudence concernant les éloignements au titre de l'article 13, lorsqu'elle est examinée conjointement avec l'article 3 (interdiction de la torture) de la CEDH, établit que les personnes faisant l'objet d'une mesure d'éloignement doivent recevoir des informations suffisantes pour garantir un accès adéquat aux procédures pertinentes et à l'aide juridique disponible, ainsi que des informations susceptibles de les aider à étayer leurs plaintes²⁵⁶. La transparence et la responsabilité dans le contexte du contrôle de l'immigration et des frontières basé sur le système AI sont donc nécessaires pour permettre aux personnes d'exercer leur droit à un recours effectif.

Pour en savoir plus

- Conseil de l'Europe, *La protection des migrants au titre de la Convention européenne des droits de l'homme et de la Charte sociale européenne*, 2013
- OSCE, *Border Management and Human Rights, Collection, processing and sharing of personal data and the use of new technologies in the counter-terrorism and freedom of movement context*, 2021, en anglais uniquement
- CEDH, *Guide de la jurisprudence - Immigration*
- EU Fundamental Rights Agency, *Handbook on European law relating to asylum, borders and immigration - Edition 2020*, 2020, en anglais uniquement
- Parlement européen, *Intelligence artificielle aux frontières de l'UE, Aperçu des applications et des questions clés*, 2021

²⁵⁴ Voir Automating Decision-making in Migration Policy: A Navigation Guide, German Marshall Fund of the United States, 2021 (*en anglais uniquement*).

²⁵⁵ *Maaouia c. France*, n° 39652/98, 5 octobre 2000, paragraphe 40 ; *Mamatkulov et Askarov c. Turquie* [GC], n°s 46827/99 et 46951/99, 4 février 2005, paragraphes 82-83 ; *M.N. et autres c. Belgique* (déc.), n° 3599/18, 5 mars 2020, paragraphe 137.

²⁵⁶ *D. c. Bulgarie*, n° 29447/17, 20 juillet 2021, paragraphe 116 ; *Hirsi Jamaa et autres c. Italie* [GC], n° 27765/09, 23 février 2012, paragraphe 204 ; *M.S.S. c. Belgique et Grèce* [GC], n° 30696/09, 21 janvier 2011, paragraphes 304-309.

- FRONTEX, [Artificial Intelligence-Based Capabilities for the European Border and Coast Guard, Final Report](#), 2021, en anglais uniquement
- EMN-OECD Inform, [The Use of Digitilisation and Artificial Intelligence in Migration Management](#), 2022, en anglais uniquement
- Conseil des droits de l'homme des Nations Unies, Report 'Impact of the use of private military and security services in immigration and border management on the protection of the rights of all migrants', 2020, UN Doc A/HRC/45/9, en anglais uniquement
- Conseil des droits de l'homme des Nations Unies, Report 'Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests', 2020, UN Doc A/HRC/44/24, en anglais uniquement
- Amnesty International, [The Digital Border: Migration, Technology and Inequality](#), 2023, en anglais uniquement
- Conseil des droits de l'homme des Nations Unies, [Digital Border Governance: a Human Rights Based Approach](#)
- ETIAS Fundamental Rights Guidance Board, [Guidance Note on right to an effective remedy and fair trial](#), en anglais uniquement
- ETIAS Fundamental Rights Guidance Board, [Guidance Note on risk for discrimination in the context of the ETIAS screening rules](#), en anglais uniquement
- European Union Agency for Fundamental Rights, [Guide on preventing unlawful profiling](#), en anglais uniquement

4.4. Processus démocratiques

140. Ce secteur comprend les activités liées à l'organisation et à l'administration des processus électoraux et des référendums, notamment l'enregistrement et la vérification des électeurs, la gestion des listes électorales, l'enregistrement des candidats, les opérations de vote, le dépouillement et le comptage des votes, la compilation et la communication des résultats, ainsi que les mécanismes de contrôle et de surveillance. Il couvre également la conception et la mise en œuvre de campagnes d'information publique, l'éducation des électeurs, la diffusion d'informations électorales et les mesures visant à garantir l'accessibilité et l'intégrité du processus électoral, y compris le recours à des services de traduction ou d'interprétation, le cas échéant. Cette section peut également s'appliquer à d'autres mécanismes participatifs formels.

Principaux cas d'utilisation de l'IA

141. Les systèmes d'IA sont utilisés, entre autres, pour soutenir, influencer, informer ou automatiser diverses étapes des cycles électoraux, des référendums et d'autres outils formels de démocratie participative.

Les cas d'utilisation comprennent :

- ***L'assistance aux électeurs grâce à l'IA*** : des 'chatbots' et des assistants virtuels fournissent des informations sur les candidats, les procédures de vote, les lieux de vote, les processus d'inscription sur les listes électorales et les projets de loi soumis à confirmation par référendum.
- ***Accessibilité électorale assistée par l'IA*** : systèmes de reconnaissance vocale permettant aux personnes malvoyantes d'accéder aux informations électorales ; traduction automatique en langue des signes ; interfaces adaptatives pour les personnes à mobilité réduite ; conversion automatique des documents électoraux en formats accessibles, notamment en braille numérique, en audio ou en langage simplifié.
- ***L'IA générative dans les campagnes politiques*** : utilisation de textes, d'enregistrements audio ou de vidéos synthétiques (tels que les 'deepfakes') à des fins de publicité politique, susceptibles d'influencer l'opinion publique ou d'imiter une communication authentique, ainsi que de systèmes basés sur l'IA pour la publicité microciblée qui segmentent les électeurs et génèrent automatiquement des messages politiques personnalisés sur les plateformes numériques.
- ***L'analyse des sentiments et l'extraction d'opinions*** : des outils qui analysent les réseaux sociaux, les actualités et les forums en ligne afin d'évaluer l'opinion publique sur les candidats, les politiques ou les questions référendaires et de fournir des informations sur les tendances émergentes.
- ***L'intégrité et la sécurité des élections*** : cela comprend les outils basés sur l'IA pour la numérisation, le dépouillement et la vérification des bulletins de vote, ainsi que les systèmes de détection des cybermenaces, des ingérences étrangères et des campagnes de désinformation coordonnées. Les outils d'IA peuvent également être utilisés pour signaler les contenus faux ou trompeurs, les « deepfakes » ou les campagnes de désinformation coordonnées ciblant les électeurs.
- ***La surveillance et le contrôle basés sur l'IA*** : des outils qui analysent la couverture médiatique, les discours sur les réseaux sociaux et les données relatives au financement des campagnes électorales afin d'identifier d'éventuelles violations de la loi ou

influences indues et de faciliter la vérification des faits en temps réel.

- **L'analyse et la prévision des données électorales** : des outils qui analysent les tendances historiques en matière de vote, les données démographiques et les tendances sociales afin de prévoir le taux de participation, d'identifier les zones où des efforts d'engagement pourraient être nécessaires et d'aider les candidats à allouer leurs ressources plus efficacement.
- **Analyse des données dans le cadre de consultations formelles** : des systèmes basés sur l'IA utilisés pour la modération de contenu, l'analyse des commentaires reçus lors de consultations publiques formelles et la recherche de consensus.

Droits humains et principes pertinents²⁵⁷

142. Les droits fondamentaux garantis par la CEDH dans ce domaine sont le droit à des élections libres (article 3 du protocole n° 1 à la CEDH) et à la liberté d'expression, qui comprend la liberté d'opinion (article 10 de la CEDH). L'utilisation de systèmes d'IA dans ce secteur peut également avoir une incidence sur la vie privée et la protection des données (article 8 de la CEDH), la non-discrimination (article 14 et protocole n° 12 à la CEDH) et le droit à un recours effectif (article 13 de la CEDH).

143. Le droit à des élections libres est un principe essentiel dans toute société démocratique et un droit individuel sur lequel toute personne ayant le droit de vote peut compter, un droit qui favorise le plus efficacement la « véritable démocratie ». ²⁵⁸ Il englobe le droit de vote et le droit de se présenter aux élections, ²⁵⁹ ainsi que le droit à la participation politique. ²⁶⁰ L'article 3 du Protocole n° 1 exige également l'existence d'un système national permettant l'examen effectif des plaintes et recours individuels en matière de droits électoraux. ²⁶¹

²⁵⁷ Dans le contexte de ce secteur, il convient de noter que la Cour a accordé une importance particulière au *Code de bonne pratique en matière électorale* de la Commission européenne pour la démocratie par le droit (Commission de Venise) et au rapport explicatif qui l'accompagne : voir par exemple *Namat Aliyev c. Azerbaïdjan*, n° 18705/06, 8 juillet 2010 ; *Riza et autres c. Bulgarie*, n°s 48555/10 et 48377/10, 13 octobre 2015 et *Cernea c. Roumanie*, n° 43609/10, 27 février 2018, *Caamaño Valle c. Espagne*, n° 43564/17, 11 mai 2021 ; *Toplak c. Slovénie* ; *Myslihaka et autres c. Albanie*, n°s 68958/17 et 5 autres, 24 janvier 2024.

²⁵⁸ Voir Cour européenne des droits de l'homme, Guide sur l'article 3 du protocole n° 1 à la Convention européenne des droits de l'homme – Droit à des élections libres

²⁵⁹ *Mathieu-Mohin et Clerfayt c. Belgique*, n° 9267/81, 2 mars 1987, paragraphes 48-51 ; *Ždanoka c. Lettonie* [GC], n° 58278/00, 16 mars 2006, paragraphe 102.

²⁶⁰ *Aziz c. Chypre*, n° 69949/01, arrêt du 22 juin 2004, paragraphe 28. Voir également la Convention des Nations Unies relative aux droits des personnes en situation de handicap, article 29 – Participation à la vie politique et publique.

²⁶¹ *Davydov et autres c. Russie*, n° 75947/11, 30 mai 2017, paragraphe 274.

144. L'article 3 du protocole n° 1 se limite au choix du pouvoir législatif. Celui-ci peut toutefois inclure d'autres instances que le parlement national, en fonction de la structure constitutionnelle du pays.²⁶² Il ne couvre généralement pas les élections locales au niveau municipal ou régional,²⁶³ à moins que l'autorité concernée n'exerce des pouvoirs législatifs tels qu'elle puisse être considérée comme faisant partie du « pouvoir législatif ».²⁶⁴ L'article 3 du protocole n° 1 ne couvre généralement pas les élections présidentielles, sauf si le président dispose de pouvoirs réels pour adopter ou bloquer des lois.²⁶⁵ En principe, les référendums ne sont pas non plus couverts.²⁶⁶ Les limites du champ d'application de l'article 3 du Protocole 1 n'excluent pas l'application d'autres droits humains et processus démocratiques pertinents aux processus qui ne relèvent pas de son champ d'application.

145. Le droit à des élections libres et à la liberté d'expression sont interdépendants et se renforcent mutuellement, formant ensemble « le fondement de tout système démocratique ».²⁶⁷ Cela implique une obligation positive pour les États membres de garantir l'existence de conditions dans lesquelles les citoyens peuvent librement se forger et exprimer leurs opinions et choisir leurs représentants. Le droit à des élections libres va au-delà du moment du vote et inclut également certains aspects de la campagne électorale. Dans certaines circonstances, le droit à des élections libres et la liberté d'expression peuvent entrer en conflit, ce qui peut inciter à juger nécessaire, avant ou pendant une élection, de prévoir certaines restrictions à la liberté d'expression, alors qu'elles ne seraient habituellement pas admissibles, afin de garantir « la libre expression de l'opinion du peuple sur le choix du corps législatif ». ²⁶⁸ Le droit à la liberté de réunion et d'association joue également un rôle

²⁶² *Timke c. Allemagne*, n° 27311/95, décision de la Commission du 11 septembre 1995.

²⁶³ *Xuereb c. Malte*, n° 17056/99, décision du 30 mai 2000 ; *Salleras Llinares c. Espagne*, n° 51882/99, décision du 29 juin 2000

²⁶⁴ *Repetto Visentini c. Italie*, n° 42081/10, décision du 19 mars 2021 ; *Miniscalco c. Italie*, n° 55093/13, décision du 17 juin 2021

²⁶⁵ *Boškosi c. l'ancienne République yougoslave de Macédoine*, n° 11676/04, décision du 3 juin 2004 ; *Brito Da Silva Guerra et Sousa Magno c. Portugal*, nos 26712/06 et 26720/06, décision du 17 juin 2008.

²⁶⁶ *Cumhuriyet Halk Partisi c. Turquie*, n° 19920/13, décision du 26 avril 2017, paragraphes 33 et 38 ; *Moohan et Gillon c. Royaume-Uni*, n° 22962/15, décision du 13 juin 2017, paragraphe 40. Toutefois, la Cour tient compte de la diversité des systèmes électoraux et n'a pas exclu la possibilité qu'un processus démocratique qualifié de « référendum » par un État contractant puisse potentiellement relever du champ d'application de l'article 3 du Protocole n° 1 (*Moohan et Gillon*, paragraphe 42).

²⁶⁷ *Bowman c. Royaume-Uni*, n° 24839/94, 19 février 1998, paragraphe 42.

²⁶⁸ *Bowman c. Royaume-Uni*, n° 24839/94, 19 février 1998 ; *Orlovskaya Iskra c. Russie*, n° 42911/08, 21 février 2017.

essentiel pour garantir le débat public, le pluralisme et le bon fonctionnement de la démocratie.²⁶⁹

146. Les États membres sont tenus de créer un environnement favorable à la participation de toutes les personnes concernées au débat public, leur permettant d'exprimer leurs opinions et leurs idées sans crainte. En vertu des articles 10 et 11 de la CEDH, l'État doit non seulement s'abstenir de toute ingérence dans les libertés d'expression, de réunion et d'association des individus, mais il a également l'obligation positive de protéger leur droit à la liberté d'expression contre toute atteinte, y compris de la part de particuliers.²⁷⁰

147. Dans certaines circonstances, il peut y avoir une tension entre la liberté d'expression (article 10 de la CEDH), la liberté de réunion et d'association (article 11 de la CEDH) et le droit à des élections libres (article 3 du protocole n° 1 de la CEDH). À cet égard, il convient de rappeler que les articles 10 et 11 autorisent la restriction de la liberté d'expression dans certaines circonstances et sous certaines conditions. Afin de garantir le caractère équitable du scrutin, certaines restrictions à la liberté d'expression peuvent être perçues comme nécessaires pendant les périodes électorales, afin de garantir la libre expression de l'opinion du peuple dans le choix du pouvoir législatif.²⁷¹ Toutefois, toute limitation doit être proportionnée à l'objectif légitime poursuivi et nécessaire dans une société démocratique. Des limites peuvent s'appliquer aux publicités politiques payantes si elles risquent de conférer des avantages injustes à des groupes puissants et de nuire à un débat ouvert et équilibré, que les États doivent protéger.²⁷²

148. L'article 5.2 de la Convention-cadre stipule que « chaque Partie adopte ou maintient des mesures qui visent à protéger ses processus démocratiques au cours des activités menées dans le cadre du cycle de vie des systèmes d'intelligence artificielle, y compris l'accès équitable et la participation des personnes au débat public, ainsi que leur capacité à se forger librement une opinion ». ²⁷³ La liberté des électeurs de se forger

²⁶⁹ Voir *Gorzeliński & Autres c. Pologne* [GC], n° 44158/98, 17 février 2004, paragraphe 88 ; *Kudrevičius & Autres c. Lituanie* [GC], n° 37553/05, 15 octobre 2015, paragraphe 142.

²⁷⁰ *Dink c. Turquie*, requêtes n°s 2668/07, 6102/08, 30079/08, 7072/09 et 7124/09, 14 septembre 2010, paragraphe 106.

²⁷¹ *Bowman c. Royaume-Uni*, n° 24839/94, 19 février 1998, paragraphe 43 ; *Orlovskaya Iskra c. Russie*, n° 42911/08, 21 février 2017, paragraphe 111.

²⁷² *Animal Defenders International c. Royaume-Uni*, n° 48876/08, arrêt du 22 avril 2013.

²⁷³ CDL-AD(2024)044-f - Déclaration interprétative du Code de bonnes pratiques en matière électorale sur les technologies numériques et l'intelligence artificielle, approuvée par le Conseil pour les élections démocratiques lors de sa 81e réunion

une opinion éclairée peut être affectée, par exemple, par les troubles de l'information en ligne, y compris la diffusion de fausses informations sur les campagnes électorales des opposants politiques. Les systèmes d'IA peuvent générer de fausses informations et exacerber la manipulation des contenus.²⁷⁴ Les outils d'IA pourraient permettre aux utilisateurs, y compris aux acteurs malveillants, de diffuser de la désinformation et des informations erronées susceptibles de compromettre l'intégrité de l'information, notamment par l'utilisation de contenus générés par l'IA ou la manipulation de contenus authentiques à l'aide de l'IA.²⁷⁵ Les 'deepfakes' politiques, à savoir la diffusion de contenus trompeurs générés par l'IA, sous forme d'audios, d'images ou de vidéos, dans le but d'influencer une élection ou de porter atteinte à la liberté des électeurs de prendre des décisions éclairées ou de répandre la haine et les préjugés, devraient être interdits et sanctionnés.²⁷⁶ Chaque fois que des systèmes d'IA ou tout autre mécanisme participatif formel sont utilisés dans le cadre d'élections, de référendums ou de tout autre mécanisme participatif formel, les électeurs doivent être informés qu'ils interagissent avec ces systèmes plutôt qu'avec un être humain.

149. Tout en reconnaissant les risques liés aux systèmes d'IA dans ce contexte, les individus ne devraient pas être soumis à une décision qui implique une restriction du contenu légal. Les systèmes d'IA peuvent aider à modérer les contenus préjudiciables sur les plateformes numériques. Cependant, il existe également un risque que la surveillance automatisée entraîne une restriction du contenu légal.²⁷⁷ Les États devraient veiller à ce que les systèmes d'IA utilisés pour la modération ou le classement ne bloquent pas le contenu légal et n'amplifient pas la désinformation d'une manière qui nuit au débat pluraliste.

150. Si les nouvelles technologies, notamment les plateformes de réseaux sociaux basées sur l'intelligence artificielle, ont permis aux partis politiques de diffuser directement des informations auprès de l'électorat, elles ont également permis à des acteurs hostiles de répandre de la désinformation et de manipuler les informations, ce qui constitue une menace importante pour la démocratie.²⁷⁸ Selon la Commission de Venise, « une nouvelle ère de désordre informationnel » a « faussé

(Venise, 5 décembre 2024) et adoptée par la Commission de Venise lors de sa 141^e session plénière (Venise, 6-7 décembre 2024).

²⁷⁴ Convention-cadre, rapport explicatif, paragraphe 44

²⁷⁵ Ibid. paragraphe 43. Voir également Note d'orientation sur la lutte contre la propagation de la mésinformation et de la désinformation en ligne par le biais de la vérification des faits et de la conception de plateformes dans le respect des droits de l'homme, Comité directeur sur les médias et la société de l'information (2023).

²⁷⁶ CDL-AD(2024)044-f, paragraphe 8.

²⁷⁷ CDL-AD(2024)044-f, paragraphe 38.

²⁷⁸ *Bradshaw et autres c. Royaume-Uni*, n° 15653/22, 22 juillet 2025, paragraphes 134-135

l'écosystème de la communication au point que les électeurs peuvent être sérieusement gênés dans leurs décisions par des informations trompeuses, manipulatrices et fausses destinées à influencer leur vote », ²⁷⁹ même s'il est difficile d'évaluer avec précision l'impact que la désinformation et les « campagnes d'influence » peuvent avoir sur les électeurs individuels et, par extension, sur le résultat d'une élection donnée. ²⁸⁰

151. Le fait qu'il soit difficile d'évaluer l'impact de la désinformation ne devrait pas empêcher les États de prendre des mesures pour défendre les valeurs démocratiques. Toutefois, si la communauté internationale s'accorde à reconnaître que l'ingérence électorale par le biais de la désinformation constitue une menace sérieuse pour la démocratie, il n'existe actuellement aucun consensus clair sur les mesures spécifiques que les États devraient prendre pour protéger leurs processus démocratiques contre ces risques, compte tenu notamment de l'importance de la liberté d'expression. ²⁸¹

152. Pour être admissibles, les restrictions doivent généralement être spécifiques au contenu. ²⁸² En principe, les interdictions générales d'exploitation de certains sites et systèmes peuvent ne pas être compatibles avec les normes électorales européennes. De même, un site ou un système de diffusion d'informations ne devrait pas être interdit de publication au seul motif qu'il pourrait critiquer le gouvernement ou le système politique et social défendu par celui-ci. Toutefois, dans le cas où un système d'IA aurait diffusé à plusieurs reprises des informations fausses dans le but d'influencer les résultats électoraux, une interdiction générale pourrait être acceptable, à condition qu'elle soit proportionnée à l'objectif légitime poursuivi et strictement nécessaire dans une société démocratique. Afin de garantir la stabilité et l'efficacité d'un système démocratique, l'État peut être amené à prendre des mesures spécifiques pour se protéger. ²⁸³ Les sanctions doivent être imposées par un organisme impartial et soumises à un système de recours efficace. ²⁸⁴

²⁷⁹ Commission de Venise, The impact of the information disorder (disinformation) on elections, CDL-LA(2018)02, paragraphe 21 (*en anglais uniquement*).

²⁸⁰ *Bradshaw et autres c. Royaume-Uni*, n° 15653/22, 22 juillet 2025, paragraphe 158. Voir également Information Disorder: Toward an interdisciplinary framework for research and policy making, rapport du Conseil de l'Europe DGI(2017)09, pp. 13-14

²⁸¹ Voir *Bradshaw*, paragraphes 159-160. Voir également paragraphes 136-138.

²⁸² CDL-AD(2024)044-f, paragraphe 60.

²⁸³ *Bradshaw et autres c. Royaume-Uni*, n° 15653/22, 22 juillet 2025, paragraphe 114

²⁸⁴ Rapport explicatif de la Convention-cadre, paragraphe 61.

153. Les États peuvent également être tenus de prévenir les inégalités dans la couverture médiatique pendant les élections.²⁸⁵ Les candidats et les partis doivent bénéficier d'un accès juste et équitable aux médias en ligne, et des réglementations devraient être mises en œuvre pour garantir que les systèmes d'IA utilisés par les intermédiaires Internet ne favorisent pas certains partis ou candidats par rapport à d'autres.²⁸⁶ Dans ce contexte, il convient de tenir dûment compte des normes générales énoncées dans [la Recommandation CM/Rec\(2022\)12 du Comité des Ministres sur la communication électorale et la couverture médiatique des campagnes électorales](#).

154. Les technologies d'IA sont également de plus en plus explorées dans le contexte du vote électronique (« e-voting »), notamment pour améliorer la sécurité du système, faciliter l'accessibilité, en particulier pour les personnes en situation de handicap, détecter les irrégularités ou aider au dépannage technique en temps réel. Le Conseil de l'Europe a établi des normes dans le domaine du vote électronique.²⁸⁷ Elles fournissent un contexte de communication propice à l'exercice du droit à des élections libres et reflètent les obligations positives de l'État de veiller à ce que les citoyens reçoivent les informations nécessaires et véridiques sur les partis politiques afin de soutenir leur choix démocratique d'élire leurs représentants. Ces normes devraient être appliquées dans le contexte du vote électronique basé sur des systèmes d'IA.

155. Si l'utilisation des technologies numériques peut rendre les processus démocratiques plus accessibles à tous les citoyens, elle peut également entraîner des obstacles et des défis pour l'exercice et le développement de la démocratie électorale. Cela vaut également pour les systèmes d'IA. Les outils électoraux basés sur l'IA doivent être conçus de manière inclusive et garantir l'accessibilité afin de permettre à tous les membres de tous les groupes, y compris les personnes en situation de handicap et les personnes âgées, de voter de manière indépendante. Dans tous les cas, des alternatives accessibles aux systèmes basés sur l'IA devraient être garanties (par exemple, des options de vote non numériques).

²⁸⁵ *Parti communiste de Russie et autres c. Russie*, n° 29400/05, 19 juin 2012, paragraphes 125 - 128.

²⁸⁶ CDL-AD(2025)003 - Rapport urgent sur l'annulation des résultats des élections par les cours constitutionnelles, publié le 27 janvier 2025, Commission de Venise. La recommandation CM/Rec(2018)2 du Comité des Ministres sur les rôles et responsabilités des intermédiaires Internet décrit les intermédiaires Internet comme des entités qui facilitent les interactions sur Internet entre les personnes physiques et morales en offrant et en assurant diverses fonctions et services (préambule, paragraphe 4).

²⁸⁷ Voir la Recommandation Rec(2004)11 du Comité des Ministres sur les normes juridiques, opérationnelles et techniques relatives au vote électronique et la recommandation CM/Rec(2017)5 sur les normes relatives au vote électronique.

Non-discrimination et égalité

156. Les États doivent veiller à ce que les systèmes d'IA utilisés lors des élections et des référendums ne conduisent pas à des résultats inégaux et discriminatoires. L'article 14 de la CEDH interdit expressément toute discrimination fondée sur « les opinions politiques ou autres ». Les États devraient se pencher sur la capacité de l'IA à générer de fausses informations ou à conduire à l'exclusion des processus démocratiques de certaines personnes ou de celles qui peuvent être sous-représentées ou se trouver dans une situation vulnérable. Les États doivent également veiller à ce que les systèmes d'IA ne restreignent ni ne découragent indirectement la participation de groupes spécifiques aux processus démocratiques.

157. Compte tenu des risques avérés de biais algorithmiques, qui peuvent également inclure l'affiliation politique, des garanties solides devraient être mises en place pour veiller à ce que ces systèmes n'excluent pas, ne désavantagent pas ou ne discriminent pas de quelque manière que ce soit certains groupes, compromettant ainsi les principes d'impartialité et de neutralité dans l'administration du processus électoral.²⁸⁸ En conséquence, tout au long du cycle de vie des systèmes d'IA dans le contexte électoral, des mesures proactives, telles que l'utilisation d'ensembles de données inclusifs et représentatifs lors de la formation des systèmes d'IA, visant à identifier et à atténuer les résultats discriminatoires devraient être mises en œuvre, afin de garantir que l'affiliation politique ou d'autres caractéristiques protégées n'affectent pas la jouissance du droit à des élections libres ou ne faussent pas le processus démocratique.

Transparence et responsabilité

158. L'existence d'un système national permettant d'examiner efficacement les plaintes et les recours individuels en matière de droits électoraux est l'une des garanties essentielles d'élections libres et équitables. Un tel système garantit l'exercice effectif des droits individuels de vote et d'éligibilité, maintient la confiance générale dans l'administration du processus électoral par l'État et constitue un moyen important pour l'État de s'acquitter de son obligation positive, en vertu de l'article 3 du protocole n°1 à la Convention, d'organiser des élections démocratiques.²⁸⁹

²⁸⁸ *Sejdić et Finci c. Bosnie-Herzégovine* [GC], n° 27996/06, 22 décembre 2009, paragraphe 44.

²⁸⁹ *Dadydov et autres c. Russie*, n° 75947/11, 30 mai 2017, paragraphe 274.

159. Lorsque des systèmes d'IA sont utilisés dans des processus démocratiques, il peut être particulièrement difficile de garantir la transparence et la responsabilité. La complexité des systèmes d'IA, qui soulève des questions d'explicabilité, et le nombre potentiellement élevé d'acteurs en amont de la chaîne d'approvisionnement rendent difficile pour les individus de détecter les violations de droits, de retracer les décisions et d'identifier les acteurs responsables. Ces difficultés sont aggravées par des problèmes de preuve. Il peut être difficile de prouver qu'un système d'IA particulier a permis une ingérence -telle que la désinformation amplifiée ou ciblée par les systèmes d'IA- qui a eu un impact concret sur le droit de vote ou d'éligibilité d'un individu. Dans la pratique, les titulaires de droits peuvent avoir du mal à démontrer comment une telle ingérence a influencé leur prise de décision ou l'intégrité globale de l'élection. Établir un lien de causalité entre l'utilisation de l'IA et la distorsion des résultats démocratiques peut nécessiter une analyse contrefactuelle que les tribunaux nationaux ne sont pas toujours en mesure de mener, en particulier lorsque les préjudices sont diffus et collectifs.

160. Les États devraient adopter ou maintenir des mesures visant à garantir la disponibilité de recours accessibles et efficaces en cas de violations des droits humains dans le cadre des processus démocratiques résultant des activités menées tout au long du cycle de vie des systèmes d'intelligence artificielle. Dans le cas spécifique des technologies électorales numériques, la recommandation CM/Rec(2017)5 du Comité des ministres sur les normes relatives au vote électronique définit les exigences en matière de responsabilité des États membres, notamment : élaborer et mettre à jour des normes techniques, d'évaluation et de certification afin de refléter les principes juridiques et démocratiques ; assurer des évaluations indépendantes des systèmes de vote électronique avant leur introduction et après des modifications importantes ; délivrer des certificats clairs qui identifient les sujets évalués et comprennent des garanties contre les modifications ; et maintenir un système d'audit ouvert et complet pour le vote électronique afin de signaler activement les problèmes potentiels.²⁹⁰ Ces mesures devraient s'appliquer de la même manière lorsque ces systèmes sont basés sur l'IA.

Droit à la vie privée et à la protection des données

161. Les systèmes d'IA utilisés dans les processus électoraux et les référendums sont intrinsèquement basés sur les données et reposent souvent sur la collecte, l'analyse et la prédiction à grande échelle de données à caractère personnel, y compris des données sensibles. Cela

²⁹⁰ Recommandation CM/Rec(2017)5 du Comité des Ministres aux États membres sur les normes relatives aux exigences de responsabilité en matière de vote électronique pour les États membres, paragraphe 36-39.

crée des risques accrus pour la protection des données et la vie privée, en particulier lorsque des informations sensibles, telles que les opinions ou affiliations politiques, sont en jeu.

162. Pour faire face à ces risques, le traitement des données à caractère personnel dans ces contextes doit être conforme aux normes de protection des données²⁹¹ et au droit au respect de la vie privée prévu à l'article 8 de la CEDH. Les données à caractère personnel concernant notamment les opinions politiques, l'appartenance syndicale et les convictions religieuses ou autres sont considérées comme une catégorie particulière de données (article 6, paragraphe 1, de la Convention 108+) et font donc l'objet d'une protection renforcée contre les risques que leur traitement peut présenter pour les droits et libertés fondamentaux de la personne concernée. Les États devraient envisager la mise en œuvre de techniques de protection de la vie privée dès la conception. La collecte de données à caractère personnel sur les opinions et les préférences des électeurs doit être limitée à ce qui est nécessaire pour les finalités définies et ne doit pas entraîner une ingérence disproportionnée dans les intérêts, les droits et les libertés des électeurs.²⁹²

Entreprises et droits humains

163. Dans le contexte de l'IA et des processus démocratiques, certains ont fait valoir que les acteurs privés, en particulier les entreprises technologiques et les intermédiaires Internet, qui comprennent les plateformes de réseaux sociaux, devraient envisager des mesures visant à soutenir les normes démocratiques et les droits humains.²⁹³ Il s'agit notamment de renforcer l'auto-évaluation et le contrôle interne pendant les périodes électorales, de coopérer avec les organismes de gestion électorale et de garantir à tous les candidats et partis politiques un accès de base aux plateformes numériques et aux outils d'IA. Il a également été suggéré de maintenir un équilibre dans la visibilité du contenu électoral, de modérer le contenu de manière responsable et d'étiqueter de manière transparente le matériel généré par l'IA et les techniques de diffusion utilisées dans les messages politiques. En outre, les plateformes

²⁹¹ Voir en particulier l'article 5 de la Convention 108(+).

²⁹² Lignes directrices sur la protection des personnes à l'égard du traitement des données à caractère personnel par et pour les campagnes politiques, Comité de la Convention 108 (T-PD) (2021).

²⁹³ Principes pour un usage conforme aux droits fondamentaux des technologies numériques dans les processus électoraux, CDL(2020)037, Commission de Venise, 2020 ; Déclaration interprétative du Code de bonne conduite en matière électorale sur les technologies numériques et l'intelligence artificielle, CDL-AD(2024)044, Commission de Venise (2024).

pourraient fournir des informations claires sur la nature politique du contenu et divulguer ses sponsors.²⁹⁴

Pour en savoir plus :

- Cour européenne des droits de l'homme, [Guide sur l'article 3 du protocole n° 1 à la Convention européenne des droits de l'homme – Droit à des élections libres](#)
- Commission de Venise, [CDL-AD\(2024\)044-e - Interpretative declaration of the Code of good practice in electoral matters as concerns digital technologies and artificial intelligence](#), 2024, en anglais uniquement
- Commission de Venise, [CDL-AD\(2025\)003 - Urgent report on the cancellation of election results by constitutional courts](#), 2024, en anglais uniquement
- Commission de Venise, [CDL-AD\(2019\)016-e - Joint Report of the Venice Commission and of the Directorate of Information Society and Action against Crime of the Directorate General of Human Rights and Rule of Law \(DGI\) on Digital Technologies and Elections](#), en anglais uniquement
- Commission de Venise, [CDL\(2020\)037 - Venice Commission Principles for a Fundamental Rights-Compliant use of Digital Technologies in Electoral Processes](#), 2020, en anglais uniquement
- Comité de la Convention 108 (T-PD), [Guidelines on the protection of individuals with regard to the processing of personal data for the purposes of voter registration and authentication](#), 2024, en anglais uniquement
- Commission de Venise, [Conclusions de la 19e Conférence européenne des administrations électorales \(EMB\) à Strasbourg et en ligne](#), 14-15 novembre 2022
- Conseil de l'Europe, [Disinformation and Electoral Campaigns](#), 2019, en anglais uniquement
- Haut-Commissariat aux droits de l'homme (OHCHR), [Human Rights and Elections. A Handbook on International Human Rights Standards on Elections](#), 2021, en anglais uniquement
- OCDE, [Facts not Fakes: Tackling Disinformation, Strengthening Information Integrity](#), 2024, en anglais uniquement
- Commission européenne, [Guidelines for providers of Very Large Online Platforms and Very Large Online Search Engines on the mitigation of systemic risks for electoral processes pursuant to Article 35\(3\) of Regulation \(EU\) 2022/2065](#), 2024, en anglais uniquement

²⁹⁴ Idem.

- Carnegie Endowment for International Peace, *Countering Disinformation Effectively: An Evidence-Based Policy Guide*, 2024, en anglais uniquement
- European Partnership for Democracy, *The EU's Artificial Intelligence Act and its Impact on Electoral Processes: a Human Rights-Based Approach*, 2024, en anglais uniquement
- International IDEA, *Artificial Intelligence for Electoral Management*, 2024, en anglais uniquement

4.5. Soins de santé

164. Les soins de santé désignent la prestation de services médicaux visant à maintenir ou améliorer le bien-être physique et mental, y compris la prévention, le diagnostic, le traitement et la réadaptation, fournis par des professionnels tels que des médecins et des infirmiers dans des contextes variés comme les hôpitaux, les cliniques, les établissements de soins primaires et les soins à domicile.

Principaux cas d'utilisation de l'IA

165. Les avancées technologiques majeures dans les systèmes d'IA ont le potentiel de faire progresser la biomédecine et de bénéficier aux soins de santé, mais leur impact et l'orientation de leurs développements sont encore incertains. Les systèmes d'IA sont développés pour une variété d'applications²⁹⁵, englobant des applications auxiliaires, telles que l'automatisation des tâches administratives de routine, mais aussi des applications ayant un impact significatif sur la fourniture de services de santé de qualité et le traitement des patients, comme l'imagerie radiologique.

166. Les principaux cas d'utilisation de l'IA sont les suivants :

- **Pose de diagnostic médical** : systèmes d'IA capables d'analyser des images médicales (radiographies, IRM, scanners, etc.), des tests de laboratoire (analyse génomique, lames, imagerie), et d'évaluer les symptômes afin d'aider à identifier les maladies et à diagnostiquer les problèmes de santé.

²⁹⁵ Pour un aperçu des applications de l'IA dans le domaine de la santé, voir Comité directeur pour les droits humains dans le domaine de la biomédecine et de la santé (CDBIO), Rapport sur l'application de l'intelligence artificielle dans les soins de santé et son impact sur la relation « patient-médecin », septembre 2024, pp. 9-11. Voir aussi : Organisation mondiale de la santé, *Éthique et gouvernance de l'intelligence artificielle pour la santé* (2021), pp. 6-16.

- **Analyse prédictive** : systèmes d'IA utilisés pour prédire les résultats des patients, tels que le risque de maladie et les complications potentielles, grâce à l'analyse des données.
- **Médecine personnalisée** : systèmes d'IA qui aident à adapter les plans de traitement à chaque patient, en optimisant les thérapies médicamenteuses et les interventions médicales grâce à l'analyse des informations génétiques et d'autres données de santé.
- **Assistants de santé virtuels** : 'chatbots' et assistants virtuels alimentés par l'IA qui apportent un soutien aux patients, notamment en matière de santé mentale, en répondant aux questions, en fixant des rendez-vous et en proposant des rappels de médicaments.
- **Télésurveillance et télémedecine** : dispositifs portables alimentés par l'IA et plateformes de télésanté permettant le suivi des patients en dehors des cadres traditionnels.
- **Chirurgie robotique** : systèmes robotiques alimentés par l'IA améliorent la précision et le contrôle des opérations chirurgicales.

Droits humains et principes pertinents

167. En vertu de l'article 8 de la CEDH, les États ont à la fois une obligation négative de ne pas interférer directement avec la santé d'un individu (sauf d'une manière justifiée par la CEDH) et une obligation positive, en vertu de l'article 8 de la CEDH, de prendre des mesures pour protéger la santé des personnes relevant de leur juridiction, selon ce qui est nécessaire et approprié dans les circonstances spécifiques. Bien que les questions de politique de santé relèvent en principe de la marge d'appréciation des États²⁹⁶, les obligations positives exigent des États qu'ils légifèrent ou mettent en œuvre des mesures pratiques pour protéger la santé et la vie des individus et veiller à ce qu'ils soient informés des risques sanitaires²⁹⁷, qu'ils établissent des réglementations obligeant les hôpitaux à protéger la vie des patients²⁹⁸, et qu'ils respectent des normes professionnelles élevées parmi les prestataires de soins de santé²⁹⁹, y compris ceux du secteur privé. La Cour a interprété l'article 8 comme couvrant le droit à la protection de l'intégrité physique, morale et psychologique, ainsi que le droit d'exercer son autonomie personnelle et son autodétermination en faisant des choix concernant son corps, y

²⁹⁶ *Vavricka et autres c. République tchèque [GC]*, n° 47621/13 et 5 autres, 8 avril 2021, paragraphes 274, 285.

²⁹⁷ *Brincat et autres c. Malte*, n° 60908/11 et 4 autres, 24 juillet 2014, paragraphe 101 ; *Guerra et autres c. Italie*, n° 116/1996/735/932, 19 février 1998, paragraphes 57-60 ; *Roche c. Royaume-Uni (GC)*, n° 32555/96, 19 octobre 2005.

²⁹⁸ *Calvelli et Ciglio c. Italie [GC]*, n° 32967/96, 17 janvier 2002, paragraphe 49 ; *Mehmet Ulusoy et autres c. Turquie*, n° 54969/09, 25 juin 2019, paragraphe 90.

²⁹⁹ *Lopes de Sousa Fernandes c. Portugal [GC]*, n° 56080/13, 19 décembre 2017, paragraphes 186-190.

compris en refusant un traitement médical ou en demandant une forme particulière de traitement médical³⁰⁰. Les autres articles à travers lesquels la Cour aborde les questions de santé sont l'article 2 (droit à la vie)³⁰¹, l'article 3 (interdiction de la torture)³⁰² et l'article 14 (interdiction de la discrimination)³⁰³. Dans sa jurisprudence concernant la santé, la Cour se réfère souvent à la Convention n° 108³⁰⁴, la Convention d'Oviedo³⁰⁵, ainsi qu'à d'autres instruments pertinents dans le cadre du Conseil de l'Europe ou au-delà³⁰⁶.

168. La CSE garantit explicitement le droit à la protection de la santé (article 11) et à l'assistance sociale et médicale (article 13). L'accès aux soins de santé est une condition préalable à la préservation de la dignité humaine.³⁰⁷ Les États doivent veiller à ce que les services de santé soient accessibles, efficaces et inclusifs en allouant des ressources suffisantes, en mettant en œuvre des procédures opérationnelles solides et en répondant aux besoins spécifiques des groupes vulnérables.³⁰⁸ L'article 11 impose trois obligations essentielles pour les États, soit directement, soit en collaboration avec des organisations publiques ou privées : (i) prendre des mesures appropriées pour éliminer autant que possible les

³⁰⁰ *Niemietz c. Allemagne*, n°13710/88, 16 décembre 1992, paragraphe 29 ; *Glass c. Royaume-Uni*, n° 61827/00, 9 mars 2004, paragraphes 74-83 ; *Tysiāc c. Pologne*, n° 5410/03, 20 mars 2007, paragraphe 107 ; *Pindo Mulla c. Espagne* [GC], n° 12345/19, 15 avril 2024, paragraphe 98 ; *Pretty c. Royaume-Uni*, n° 2346/02, 29 avril 2002, paragraphe 63 ; *Taganrog LRO et autres c. Russie*, n° 32401/10 et 19 autres, 7 novembre 2019, paragraphe 162.

³⁰¹ *Centre de ressources juridiques pour le compte de Valentin Campeanu c. Roumanie* [GC], n° 47848/08, 17 juillet 2014, paragraphes 145-147 ; *Oyal c. Turquie*, n° 4864/05, 23 mars 2010, paragraphe 72.

³⁰² *Paposhvili c. Belgique* [GC], n° 41738/10, 13 décembre 2016, paragraphes 183-193 ; *D. c. Royaume-Uni*, n° 30240/96, 2 mai 1997, paragraphe 54 ; *Aswat c. Royaume-Uni*, n° 17299/12, 16 avril 2013, paragraphes 55-57.

³⁰³ *Kiyutin c. Russie*, n° 2700/10, 10 mars 2011, paragraphes 56-58, 74

³⁰⁴ Par exemple, *S. et Marper c. Royaume-Uni* [GC], 2008, paragraphes 41 et 103.

³⁰⁵ *Glass c. Royaume-Uni*, 2004, paragraphe 58. La « Convention d'Oviedo » désigne la Convention pour la protection des droits de l'homme et de la dignité de l'être humain à l'égard des applications de la biologie et de la médecine : Convention sur les droits de l'homme et la biomédecine, Oviedo, 4 avril 1997 (STE n° 164). La Convention d'Oviedo est complétée par quatre protocoles additionnels. Voir <https://www.coe.int/en/web/human-rights-and-biomedicine/oviedo-convention>

³⁰⁶ Par exemple, voir la référence dans *Biriuk c. Lituanie* (n° 23373/03, 25 novembre 2008, paragraphe 21) à la Recommandation n° R (89) 14 du Comité des Ministres du Conseil de l'Europe sur « Les incidences éthiques de l'infection VIH dans le cadre sanitaire et social » (1989) ou la référence dans *Pindo Mulla c. Espagne*, (GC) n°15541/20, 17 septembre 2024, paragraphe 77, à la Déclaration universelle sur la bioéthique et les droits de l'homme adoptée par l'UNESCO en 2005.

³⁰⁷ *Fédération internationale pour les droits humains (FIDH) c. France*, n° 14/2003, 3 novembre 2004, paragraphe 31.

³⁰⁸ Déclaration d'interprétation sur le droit à la protection de la santé en cas de pandémie, 21 avril 2020.

causes de maladie ; (ii) mettre en place des services consultatifs et éducatifs pour promouvoir la santé et encourager la responsabilité individuelle; et (iii) prendre des mesures pour prévenir autant que possible les maladies épidémiques, endémiques et autres, ainsi que les accidents. Les États sont en outre tenus de protéger les groupes vulnérables³⁰⁹, tels que les sans-abris, les personnes âgées, les personnes en situation de handicap et les personnes en situation migratoire irrégulière, en veillant à ce que leur droit à la santé ne soit pas entravé, même par des conditions restrictives. En outre, les étrangers sont ressortissants d'autres Parties résidant ou travaillant légalement sur le territoire d'une Partie ont droit à la protection de la santé en vertu de la CSE.

Droit à la vie privée et à la protection des données

169. Comme indiqué dans la section consacrée aux [questions fondamentales relatives aux droits humains dans les secteurs de la gouvernance publique](#), l'article 8 de la CEDH protège les données à caractère personnel liées à la santé³¹⁰, qui constituent un élément clé de la vie privée. L'article 10 de la Convention d'Oviedo stipule que toute personne a : a) droit au respect de sa vie privée s'agissant des informations relatives à sa santé et b) droit de connaître toute information collectée sur sa santé. Les données personnelles relatives à la santé sont explicitement considérées comme sensibles en vertu de la Convention 108 (article 6) ainsi que des cadres réglementaires régionaux et nationaux³¹¹. Le Comité des Ministres du Conseil de l'Europe a publié des lignes directrices spécifiques sur la protection des données relatives à la santé dans sa [Recommandation CM/Rec\(2019\)2](#), qui vise à garantir que les principes de la Convention n° 108, y compris sa version modernisée, sont pleinement appliqués à l'échange et au partage des données relatives à la santé.

170. Les systèmes d'IA dans le domaine de la santé peuvent s'appuyer fortement sur des données sensibles relatives aux patients, notamment des dossiers médicaux et des informations biométriques, tant pour leur formation, leurs tests et leur validation que lorsqu'ils sont utilisés dans le cadre de la prise de décision et de la prévision. La sécurité des données, la confidentialité et l'utilisation abusive potentielle, comme les violations

³⁰⁹ *Commission internationale de juristes (CIJ) et Conseil européen pour les réfugiés et les exilés (ECRE) c. Grèce*, réclamation n° 173/2018, décision sur le fond du 26 janvier 2021, paragraphe 218.

³¹⁰ *Surikov c. Ukraine*, n° 42788/06, 26 janvier 2017, paragraphes 70 et 89.

³¹¹ Voir, par exemple, les articles 4 et 9 et les considérants 35 et 53 du RGPD, qui définissent les termes « données relatives à la santé », « données génétiques » et « données biométriques ».

ou le partage non autorisé, font partie des préoccupations³¹². En outre, les individus peuvent être confrontés à des difficultés pour exercer un contrôle sur leurs données, en particulier lorsqu'elles sont incluses dans des ensembles de données d'entraînement à l'IA. La divulgation de données sur la santé peut avoir de profondes répercussions sur la vie privée et familiale, ainsi que sur la situation sociale et professionnelle, avec un risque de stigmatisation et d'exclusion. C'est pourquoi les législations nationales doivent prévoir des garanties pour empêcher le partage ou la divulgation non autorisés, afin de respecter les garanties de l'article 8³¹³.

Non-discrimination et accès équitable aux soins de santé

171. Comme indiqué dans la section consacrée aux [questions fondamentales relatives aux droits humains dans les différents secteurs de la gouvernance publique](#), la CEDH et la CSE interdisent la discrimination.³¹⁴ En vertu de l'article 3 de la convention d'Oviedo, les États parties sont tenus de prendre les mesures appropriées en vue d'assurer, dans les limites de leur juridiction, un accès équitable à des soins de santé de qualité appropriée³¹⁵.

172. Les biais dans les données utilisées pour développer et entraîner les systèmes d'IA peuvent fausser l'évaluation des besoins de santé et des traitements des patients. Il est à noter que les modèles d'IA formés principalement à partir de données provenant de populations spécifiques peuvent poser des diagnostics erronés ou sous-estimer la gravité de la maladie dans les groupes sous-représentés tels que les femmes et les filles, les personnes appartenant à des minorités ethniques, les populations autochtones, les personnes âgées ou les personnes en situation de handicap³¹⁶. On peut citer comme exemples les systèmes de

³¹² Voir également le rapport du CDBIO sur le rôle des professionnels de la santé et des prestataires de soins de santé dans la collecte, la génération et l'enrichissement, ainsi que dans la sauvegarde des données de santé (*Report on the role of health professionals and healthcare providers in collecting, generating and enriching*), pp. 21-23, qui fait référence à une décision rendue en 2017 par l'Information Commissioner's Office (ICO) du Royaume-Uni, constatant une violation de la loi applicable en matière de protection des données et du droit à la vie privée dans le cas d'un établissement de soins de santé ayant accordé à une société privée l'accès à plus d'un million de fichiers de données de patients pseudonymisés afin de tester un système d'intelligence artificielle en cours de développement.

³¹³ *Z. c. Finlande*, n° 22009/93, 25 février 1997, paragraphe 95.

³¹⁴ Voir le préambule de l'année 1961 de la CSE et la partie V-article E de la Charte sociale européenne révisée.

³¹⁵ Voir également les articles 15 paragraphe 1(b) et 2 paragraphe 2 du Pacte international relatif aux droits économiques, sociaux et culturels (PIDESC) sur le droit de toute personne de bénéficier des progrès scientifiques et de leurs applications, sans discrimination d'aucune sorte.

³¹⁶ Voir par exemple le rapport du CDBIO, p. 26 ; voir également OMS, *Ethics and governance of artificial intelligence for health* (2021), pp. 54-57. En outre, sur la sous-

hiérarchisation des greffes de rein, où des données historiques biaisées ont faussé les résultats au détriment de certains patients.³¹⁷ De même, une représentation inadéquate dans les ensembles de données de formation a conduit à des diagnostics erronés d'affections cutanées³¹⁸. En outre, on craint que l'accès aux avantages offerts par l'IA dans le domaine des soins de santé ne soit pas également disponible pour tous. Le déploiement de ces soins peut être inégal sur le plan géographique dans un pays donné, ou dépendre des moyens financiers des patients³¹⁹. Le manque d'accessibilité des applications d'IA peut exclure les personnes âgées ou les personnes en situation de handicap. Les États devraient adopter des mesures visant à garantir que les systèmes d'IA soient développés et déployés de manière équitable.

Consentement éclairé, autonomie et prise de décision

173. Le consentement éclairé et l'autonomie de décision du patient³²⁰ sont garantis par l'article 8 de la CEDH³²¹ et l'article 11 de la CSE³²². L'article 5 de la convention d'Oviedo exige un consentement libre et éclairé

représentation et la faible qualité des données des femmes, ainsi que des personnes de divers genres dans la recherche scientifique, l'étude GEC/CDADI, p. 25. Également (p. 26) sur la discrimination structurelle intégrée dans les systèmes d'IA à l'égard des patients systématiquement défavorisés issus de minorités ethniques. Voir également de l'OMS : *Ageism in artificial intelligence for health* (2022), qui montre que les systèmes algorithmiques utilisés dans le secteur de la santé sont entraînés sur les données de populations majoritairement jeunes, ce qui entraîne des performances disproportionnellement plus faibles de ces systèmes pour les patients plus âgés, y compris des diagnostics erronés www.who.int/publications/i/item/9789240040793.

³¹⁷ Voir, par exemple (en anglais uniquement) : www.wired.com/story/how-algorithm-blocked-kidney-transplants-black-patients ; <https://algorithmwatch.org/en/racial-health-bias-switzerland>.

³¹⁸ Voir, par exemple (en anglais uniquement) : www.theguardian.com/society/2021/nov/09/ai-skin-cancer-diagnoses-risk-being-less-accurate-for-dark-skin-study

³¹⁹ Rapport CDBIO, p. 26. Concernant la discussion sur la possibilité que la fracture numérique existante (y compris en ce qui concerne l'IA) et les inégalités (au sein des pays et entre eux, ainsi qu'entre les groupes sociaux) exacerbent la répartition inégale des soins de santé et les problèmes d'accès effectif aux soins de santé, voir la recommandation PACE 2185 (2020), *Intelligence artificielle et santé : défis médicaux, juridiques et éthiques* à venir. Une préoccupation supplémentaire pourrait être liée à l'utilisation de l'IA pour l'allocation des ressources et la hiérarchisation des cas.

³²⁰ L'autonomie va au-delà du consentement éclairé et engendre un rôle plus actif pour le patient dans la prise de décision partagée, englobant, par exemple, le choix de prendre des mesures préventives, de demander un deuxième avis ou d'introduire ses propres valeurs, préférences et perspectives dans les communications patient-médecin (Rapport CDBIO p. 13).

³²¹ *Trocellier c. France* (déc.), n° 75725/01, 13 avril 2007, paragraphe 4 ; *Mayboroda c. Ukraine*, n° 14709/07, paragraphe 52.

³²² *Transgender Europe et ILGA Europe c. République tchèque*, plainte n° 117/2015, 15 mai 2018, paragraphe 81.

pour les interventions sanitaires, avec une information préalable sur l'objectif, les risques et les conséquences. Le consentement peut être retiré à tout moment. Une attention particulière est accordée aux situations d'urgence et aux personnes incapables de donner leur consentement³²³.

174. Les individus doivent pouvoir donner ou refuser librement leur consentement à toute intervention, comprenant tous les actes médicaux, y compris ceux effectués à des fins de soins préventifs, de diagnostic, de traitement, de rééducation ou de recherche. Leur consentement est considéré comme libre et éclairé lorsqu'il est donné sur la base d'informations objectives et complètes fournies par le professionnel de santé responsable, qui répond notamment de manière adéquate aux demandes d'informations complémentaires. Les informations fournies doivent être suffisamment détaillées pour que le patient comprenne la portée, les domaines et les étapes de l'utilisation des outils d'IA. La nature « boîte noire » de nombreux systèmes d'IA qui produisent des résultats probabilistes rend difficile la compréhension et l'évaluation de la nécessité ou de l'utilité de l'intervention. Des exigences adéquates en matière de transparence et de contrôle des systèmes d'IA et leurs développeurs, ainsi que la formation des médecins qui les utilisent, pourraient atténuer ce problème. Les préoccupations relatives à la « déqualification » des professionnels de santé et à la dépersonnalisation de la relation patient-médecin méritent une attention particulière.³²⁴

Pour en savoir plus

- [Recommandation CM/Rec \(2019\)2](#) du Comité des Ministres aux États membres sur la Protection des données relatives à la santé
- Assemblée parlementaire du Conseil de l'Europe, [L'intelligence artificielle dans les soins de santé : défis médicaux, juridiques et éthiques à venir](#), Recommandation 2185, 2020
- Comité directeur pour les droits humains dans les domaines de la biomédecine et de la santé (CD-BIO), [Rapport sur l'application de l'intelligence artificielle dans les soins de santé et son impact sur la relation 'patient-médecin'](#), 2024
- Brent Mittelstadt, chercheur principal et directeur de recherche à l'Oxford Internet Institute, Université d'Oxford, Royaume-Uni,

³²³ Articles 6 à 8. Voir également le rapport explicatif de la convention d'Oviedo, paragraphes 35-36.

³²⁴ Conformément à l'article 4 de la Convention d'Oviedo, toute intervention dans le domaine de la santé doit être effectuée dans le respect des obligations et des normes professionnelles pertinentes. Cela est interprété comme une obligation pour les professionnels de la santé de prêter une attention particulière aux besoins spécifiques de chaque patient. Voir les paragraphes 32 et 33 du rapport explicatif de la Convention d'Oviedo.

- Rapport de l'expert consultant sur l'impact de l'intelligence artificielle sur la relation médecin-patient, en anglais uniquement
- Comité directeur pour les droits humains dans les domaines de la biomédecine et de la santé (CD-BIO), *Plan d'action stratégique sur les droits de l'homme et les technologies en biomédecine (2020-2025)*, 2019
 - Ivana Bartoletti et Raphaële Xenidis, Conseil de l'Europe, *Étude sur l'impact des systèmes d'intelligence artificielle, leur potentiel pour promouvoir l'égalité, y compris l'égalité entre les sexes, et les risques qu'ils peuvent présenter en matière de non-discrimination*, 2023
 - Organisation mondiale de la santé (OMS), *Ethics and governance of artificial intelligence for health*, 2021, en anglais uniquement
 - Organisation mondiale de la santé (OMS), *Ageism in artificial intelligence for health*, 2022, en anglais uniquement
 - Organisation mondiale de la santé (OMS), *Regulatory considerations on artificial intelligence for health*, 2023
 - Organisation mondiale de la santé (OMS), *Ethics and governance of artificial intelligence for health, Guidance on large multi-modal models*, 2024, en anglais uniquement
 - Programme des Nations unies pour l'environnement, *Navigating New Horizons, Rapport prospectif mondial sur la santé planétaire et le bien-être humain*, 2024, en anglais uniquement
 - Mental Health Europe, *Study on Artificial Intelligence in mental healthcare*, 2025, en anglais uniquement
 - OCDE, *AI in Health: Huge Potential, Huge Risks*, 2024, en anglais uniquement.

4.6. Services sociaux et protection sociale

175. Les services sociaux englobent un large éventail de programmes et de services visant à garantir un niveau de vie minimum et à promouvoir le bien-être humain et social. Outre les services publics fondamentaux tels que les soins de santé et l'éducation, qui sont traités spécifiquement dans les parties 4.5 et 4.7 respectivement du présent Manuel, les services sociaux et les systèmes de protection sociale offrent des avantages tant financiers que non financiers. Il s'agit notamment des programmes de sécurité sociale qui offrent un soutien financier aux personnes âgées, aux personnes en situation de handicap et aux survivants ; des prestations de maladie et d'accident ; des allocations chômage ; des allocations maternité et paternité, des allocations familiales, des aides au logement (subventions ou logements sociaux) et des aides aux sans-abri ou aux personnes menacées de le devenir ; du revenu minimum garanti ou des prestations en nature, telles que l'aide alimentaire aux familles à faibles revenus ; les services à l'enfance et à la famille, y compris les subventions pour la garde d'enfants, les programmes et outils visant à lutter contre la

violence domestique et les services de protection de l'enfance ; le soutien aux personnes âgées et aux personnes en situation de handicap.

Principaux cas d'utilisation de l'IA

176. L'IA est de plus en plus intégrée aux services sociaux, allant de l'automatisation des tâches de routine telles que la prise de notes et la gestion des dossiers à des applications plus complexes ayant un impact significatif. Les principales fonctions basées sur l'IA sont les suivantes :

- **Analyse prédictive** : systèmes d'IA capables d'analyser de grands ensembles de données à l'aide de processus algorithmiques, y compris l'apprentissage automatique, pour identifier les individus ou les groupes les plus susceptibles d'avoir besoin de services sociaux. Cela permet aux agences d'allouer de manière proactive le soutien et les ressources, par exemple en identifiant les enfants à risque qui pourraient avoir besoin d'une aide supplémentaire.
- **Allocation des ressources** : modèles basés sur l'IA optimisant la distribution de ressources généralement limitées, garantissant une prestation de services plus efficace et plus équitable.
- **Filtrage et détection des fraudes** : systèmes d'IA utilisés pour aider à filtrer les candidats, vérifier leurs informations, signaler les incohérences et identifier les schémas révélateurs de fraude ou d'utilisation abusive des services sociaux, améliorant ainsi la responsabilité et l'efficacité.
- **Les « chatbots » et les assistants virtuels pilotés par l'IA** : systèmes traitant les demandes de routine, améliorant l'accessibilité pour les personnes en situation de handicap grâce à la reconnaissance vocale ou à la transcription automatique, et surveillant la santé physique et mentale des individus, en émettant des alertes pour assurer des interventions en temps utile.
- **Vue d'ensemble et évaluation** : l'IA analyse les résultats des services sociaux pour évaluer leur efficacité, en fournissant des informations basées sur des données qui aident les agences à affiner leurs politiques et à améliorer la prestation de services au fil du temps.

Droits humains et principes pertinents

177. La fourniture de services sociaux peut interférer directement avec la jouissance par un individu de ses droits, tels que le droit à la vie familiale au sens de l'article 8 de la CEDH³²⁵, le droit à la liberté au sens de l'article

³²⁵ Par exemple, en ce qui concerne les décisions relatives au déplacement des enfants, au placement et à l'adoption, à la détermination du droit de garde et du droit

5³²⁶, ou le droit à la propriété au sens de l'article 1 du Protocole n° 1³²⁷. En outre, des services sociaux efficaces contribuent à l'accomplissement des obligations positives de l'État en matière de prévention des mauvais traitements administrés par des personnes privées (article 3)³²⁸.

178. Les États disposent d'une marge d'appréciation dans les domaines impliquant l'application de politiques sociales ou économiques³²⁹. En outre, la Cour respecte généralement les choix politiques nationaux, à moins qu'ils ne soient « manifestement dépourvu de base raisonnable »³³⁰. C'est particulièrement le cas dans le contexte de l'allocation des ressources limitées de l'État³³¹. La Cour a ainsi estimé qu'il était légitime pour les États de mettre en place des critères selon lesquels une prestation peut être attribuée, lorsque l'offre est insuffisante pour satisfaire la demande, pour autant que ces critères ne soient pas arbitraires ou discriminatoires³³². Cela signifie que lorsqu'un État décide

de visite, voir *B. c. Royaume-Uni*, 8 juillet 1987, n° 9840/82, paragraphes 60-65 ; *Saviny c. Ukraine*, 18 décembre 2008, 39948/06, paragraphes 57-42 ; *A.K. et L. c. Croatie*, 8 janvier 2013, 37956/11, paragraphes 58-60. Voir aussi, pour les obligations des autorités nationales de faciliter les visites familiales et, dans des cas exceptionnels, d'assurer un abri aux personnes particulièrement vulnérables, *A et autres c. Italie*, 7 décembre 2003, 17791/22, paragraphes 93-104.

³²⁶ Par exemple, en ce qui concerne l'internement obligatoire des personnes présentant « un trouble mental ». Voir, entre autres, *Ilmseher c. Allemagne* [GC], 4 décembre 2018, n° 10211/12 et 27505/14, paragraphes 126-134.

³²⁷ Pour une synthèse complète de la jurisprudence de la Cour relative à la sécurité sociale/aux prestations sociales, voir *Béláné Nagy c. Hongrie* [GC], 13 décembre 2016, n° 53080/13, paragraphe 80-89 ; *Yavaş et autres c. Turquie*, n° 36366/06, 5 mars 2019, 36366/06, paragraphes 39-43.

³²⁸ Voir, entre autres, *Z. et autres c. Royaume-Uni*, 10 mai 2001, n° 29392/95, paragraphe 121, concernant le manquement des services sociaux de l'Etat défendeur à prendre des mesures de protection adéquates dans un cas de maltraitance d'enfant, ainsi que *V.C. c. Italie*, 1^{er} février 2018, n° 54227/14, paragraphe 89. De même, en ce qui concerne l'absence de protection des victimes de violence domestique, voir *Opuz c. Turquie*, 9 juin 2009, n° 33401/02, paragraphe 159 ; *Talpis c. Italie*, 2 mars 2017, n° 41237/14, paragraphe 141, également en liaison avec l'article 14 et l'absence de garantie par l'État du droit des femmes à une égale protection devant la loi.

³²⁹ Par exemple, en ce qui concerne le logement, voir, entre autres, *Hudorovič et autres c. Slovaquie*, 10 mars 2020, nos 24816/14 et 25140/14 et *Forum européen des Roms et des Gens du voyage (ERTF) c. France*, n° 64/2011, 24 janvier 2012, paragraphe 95 ; concernant les pensions de vieillesse, *Fábián c. Hongrie*, 5 septembre 2017, n° 78117/13, paragraphe 67 ; concernant les pensions de réversion, *Muñoz Díaz c. Espagne*, 8 décembre 2009, n° 49151/07, paragraphes 48-49, etc. ; concernant les politiques de l'emploi, voir, *Fédération générale des employés de la société nationale d'électricité (GENOP-DEI) / Confédération des syndicats de fonctionnaires grecs (ADEDY) c. Grèce*, n° 66/2011, 23 mai 2012, paragraphe 20.

³³⁰ *Stec et autres c. Royaume-Uni* [GC], 12 avril 2006, nos 65731/01 et 65900/01, paragraphe 52

³³¹ *Saltinytė c. Lituanie*, 26 octobre 2021, n° 32934/19, paragraphes 64 et 77.

³³² *Bah c. Royaume-Uni*, 27 décembre 2011, n° 56328/07, paragraphe 52

d'accorder de telles prestations, il doit le faire de manière non discriminatoire. La marge d'appréciation de l'État est considérablement réduite lorsque la distinction de traitement est fondée sur une caractéristique personnelle inhérente ou immuable telle que la race, le sexe, la nationalité ou le handicap, et des « considérations très fortes » seraient nécessaires pour justifier la différence de traitement en question³³³.

179. En vertu de la CSE, les États parties ont l'obligation de garantir un accès non discriminatoire à la sécurité sociale³³⁴, à l'assistance sociale et médicale³³⁵ et aux services de protection sociale³³⁶. Cela implique que le système de sécurité sociale garantisse un accès effectif aux prestations prévues dans chaque branche du système concerné³³⁷. L'égalité de traitement doit être assurée aux ressortissants d'autres États parties résidant légalement ou travaillant régulièrement sur le territoire de l'État partie concerné, ainsi qu'aux réfugiés et aux apatrides.³³⁸

Droit à la vie privée et à la protection des données

180. L'utilisation de l'IA dans les services sociaux implique le traitement de données personnelles sensibles, ce qui soulève de sérieuses préoccupations en matière de respect de la vie privée au titre de l'article 8 de la CEDH. L'agrégation de données sensibles, telles que les dossiers médicaux, les antécédents financiers et professionnels et d'autres détails personnels, qui permet à l'État d'acquérir un profil détaillé des aspects les plus intimes de la vie des citoyens, peut entraîner une ingérence particulièrement envahissante dans la vie privée³³⁹. Par exemple, des préoccupations liées au respect de l'article 8 de la CEDH ont été soulevées dans l'affaire « SyRi », où le tribunal de district de La Haye a estimé qu'un algorithme utilisé pour identifier les fraudes potentielles à l'aide sociale (le 'Systeem Risico Indicatie' ou 'SyRi') et la législation

³³³ *Savickis et autres c. Lettonie* [GC], 9 juin 2022, n° 49270/11, paragraphe 83 ; *J.D. et A. c. Royaume-Uni*, 24 octobre 2019, n° 32949/17, n° 34614/17, paragraphes 88-89, 97 et 104 ; *Andrejeva c. Lettonie* [GC], 18 février 2009, n° 55707/00, paragraphe 87 ; *Ribač c. Slovaquie*, 5 mars 2018, n° 57101/10, paragraphe 53.

³³⁴ CSE, article 12 ; voir également le Digest of Case Law of the European Committee of Social Rights du Comité européen des droits sociaux, décembre 2022, p. 119 et suivantes.

³³⁵ CSE, article 13.

³³⁶ CSE, article 14.

³³⁷ Digest of Case Law of the European Committee of Social Rights, décembre 2022, p. 120.

³³⁸ CSE, article 12, paragraphe 4 ; paragraphe 1 de l'annexe de la CSE.

³³⁹ *Szabó et Vissy c. Hongrie*, n° 37138/146, 12 janvier 2016, paragraphe 70.

correspondante ne répondaient pas aux exigences de nécessité et de proportionnalité requises par l'article 8, paragraphe 2, de la CEDH³⁴⁰.

181. Un risque supplémentaire est l'utilisation abusive des données personnelles collectées dans les services sociaux, y compris la surveillance non autorisée, le profilage sans consentement, ou les violations accidentelles. L'implication des entreprises dans le développement ou la maintenance des systèmes d'IA ou l'externalisation des services sociaux auprès d'entreprises privées suscitent également des inquiétudes. Étant donné que les systèmes d'IA stockent de grandes quantités de données sensibles, il convient d'accorder une importance particulière à la sécurité des données, y compris lorsqu'un système d'IA particulier est développé et entretenu par des fournisseurs tiers (privés).

Non-discrimination et égalité

182. L'utilisation de l'IA dans les services sociaux peut perpétuer la discrimination (y compris indirecte et intersectionnelle) en raison des préjugés intégrés dans les données sociétales, tels que les préjugés raciaux, sexistes ou socio-économiques.³⁴¹ Cela peut entraîner un refus injustifié de services ou de prestations, affectant de manière disproportionnée les groupes marginalisés et compromettant l'accès égal à ces services. Les systèmes d'analyse prédictive, de détection d'erreurs ou de fraudes, ainsi que les systèmes d'allocation des ressources, sont plus susceptibles d'être affectés par des biais, car ils reposent sur des données historiques et risquent d'aggraver la discrimination structurelle et les stéréotypes. Par exemple, un système de détection de fraude formé sur des données qui reflètent de manière disproportionnée les expériences de certains groupes est susceptible de développer des profils de risque et d'établir des liens basés sur des biais, tels que le statut socio-économique faible ou un passé migratoire. Cela peut entraîner des recommandations biaisées et, finalement, la violation du droit à la non-discrimination, non seulement pour les individus, mais aussi pour l'ensemble des populations perçues par le système comme homogènes.

³⁴⁰ The Hague District Court, *NCJM et al. and FNV v The State of the Netherlands*, 6 mars 2020, disponible en anglais sur : uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:1878 (ECLI:NL:RBDHA:2020:865). Il s'agit du 'Systeem Risico Indicatie' ou 'SyRi'. Voir également le mémoire d'*amicus curiae* présenté par le Rapporteur spécial des Nations Unies sur l'extrême pauvreté et les droits humains, qui souligne en particulier l'effet discriminatoire et stigmatisant du SyRi. <https://www.ohchr.org/sites/default/files/Documents/Issues/Poverty/Amicusfinalversionsigned.pdf> (en anglais uniquement)

³⁴¹ Voir *Pays-Bas – Avis sur la protection juridique des citoyens*, CDL-AD(2021)031, Commission de Venise, 2021, paragraphes 96-98 [https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD\(2021\)031-f](https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2021)031-f)

Des mesures de protection sont nécessaires, y compris la surveillance humaine, afin de garantir l'évaluation critique des résultats de l'IA et ainsi neutraliser le risque d'effets discriminatoires³⁴².

183. En cas d'allégation de discrimination, les autorités nationales devraient prendre toutes les mesures raisonnables pour déterminer si le résultat était discriminatoire. Cela devrait inclure une enquête efficace et indépendante.³⁴³

Transparence et responsabilité

184. Comme nous l'avons déjà observé, les processus décisionnels de l'IA peuvent être opaques, de sorte qu'il est difficile de comprendre comment et pourquoi une décision a été prise. Ce manque de transparence peut nuire à la responsabilité dans la prestation des services sociaux, en particulier lorsque des personnes se voient refuser des prestations ou des services sur la base de décisions de l'IA. Si une personne est désavantagée par une décision d'IA (par exemple, si elle se voit refuser à tort des prestations sociales), il peut être difficile pour elle de faire appel ou de contester la décision en raison de la nature « boîte noire » de nombreux systèmes d'IA, que ce soit intentionnel (c'est-à-dire pour des considérations de propriété intellectuelle) ou intrinsèque (c'est-à-dire trop compliqué pour quelqu'un qui n'a pas de compétences numériques particulièrement poussées).

185. Le manque de transparence et de responsabilité dans l'utilisation des systèmes d'IA peut priver les personnes concernées par les décisions prises par l'IA d'une explication ou de la possibilité de faire appel contre des décisions qui, dans certains cas, peuvent être d'une importance vitale pour elles, et porter ainsi atteinte à leur droit à un recours effectif. Dans les cas où les événements en question relèvent entièrement, ou en grande partie, de la connaissance exclusive des autorités, comme ce serait sans doute le cas lorsque des systèmes d'IA sont impliqués, ou lorsqu'il serait extrêmement difficile en pratique pour le demandeur de prouver la

³⁴² Il convient toutefois de noter que l'implication humaine ne suffit pas à elle seule à neutraliser les risques de discrimination ; dans le scandale des allocations familiales néerlandaises, par exemple, les fonctionnaires étaient chargés d'examiner manuellement les demandes présentant le score de risque le plus élevé. Sans d'informations sur les raisons pour lesquelles le système avait attribué un score de risque élevé à une demande spécifique, les fonctionnaires avaient tendance à généraliser le comportement des individus de la même race ou de la même ethnie, les percevant de manière stéréotypée comme frauduleux ou déviants.

³⁴³ *Basu c. Allemagne*, n°. 215/19, 18 octobre 2022, paragraphe 38.

discrimination, la Cour/ le CEDS a déplacé la charge de la preuve sur les autorités³⁴⁴.

Accessibilité et qualité des soins

186. Les personnes en situation de vulnérabilité telles que les personnes âgées, les personnes en situation de handicap ou celles dont la culture numérique ou l'accès aux technologies modernes sont limités, peuvent être mal équipées pour interagir avec les systèmes d'IA. Ces groupes peuvent rencontrer des difficultés pour accéder aux services basés sur l'IA, qu'il s'agisse de simples plateformes d'application en ligne, de 'chatbots' ou d'assistants virtuels. Cela pourrait entraîner l'exclusion des services sociaux et, par conséquent, exacerber les inégalités existantes.

187. À l'autre bout du dispositif de prestation des services sociaux, la dépendance aux systèmes d'IA soulève des questions liées à la qualité. De tels systèmes sont, dans la plupart des cas, conçus pour soutenir les décisions des professionnels humains et ne doivent pas remplacer le jugement humain. Néanmoins, comme le montre la jurisprudence nationale, il peut exister des cas où les professionnels manquent de temps, de ressources ou sont tout simplement sujets à un biais d'automatisation, et réticents à utiliser leur expertise professionnelle pour prendre une décision différente de celle recommandée par le système. Cependant, les systèmes d'IA ne sont pas infaillibles³⁴⁵, et les erreurs dans les allocations peuvent être fatales pour certains des membres les

³⁴⁴ *Salman c. Turquie* [GC], n° 21986/93, 27 juin 2000, n° 21986/93, paragraphe 100 ; *Anguelova c. Bulgarie*, n° 8361/97, 13 juin 2002, 38361/97 paragraphe 111 ; n° 3891/19, *Cînta c. Roumanie*, 18 février 2020, n° 3891/19, paragraphe 79 ; *Mental Disability Advocacy Centre (MDAC) c. Bulgarie*, n° 41/2007, 3 juin 2008, paragraphe 52.

³⁴⁵ Par exemple, au Royaume-Uni, l'arrêt *Johnson et autres c. SSWP* (EWCA Civ 778, *Judgement, Secretary of State for Work et Pensions c Johnson et al, Affaires nos : CO/1643/2018 CO/1552/2018*, <https://www.judiciary.uk/wp-content/uploads/2019/01/johnson-and-others-judgment-final.pdf>) a soulevé d'importantes questions découlant de la mise en œuvre d'un système d'IA prenant des décisions en matière de prestations et d'aide sociale pour le système alors nouvellement introduit du crédit universel (un paiement unique d'aide sociale comprenant un montant personnel de base reflétant également les besoins en matière de garde d'enfants, de logement et d'autres besoins prescrits). Les demandeurs ont fait valoir que le système d'évaluation automatisé utilisé pour calculer le montant du crédit universel payable à chaque demandeur était illégal et pouvait créer une insécurité des revenus, tandis que l'État a reconnu que la méthode était "malheureuse" et "arbitraire", mais que la refonte du système « à partir de zéro » pour tenir compte des ajustements serait trop onéreuse. Cette défense a été rejetée et la contestation a abouti, au motif que les effets, dans ces cas, ont été jugés contraires à la politique et aux objectifs des règlements sous-jacents de l'UC et donc « irrationnels ».

plus vulnérables de la société. De plus, il existe une inquiétude selon laquelle les services sociaux « numériques par conception » et la dépendance excessive à l'IA conduiraient à l'érosion des compétences des travailleurs sociaux, compromettant ainsi la qualité du service, notamment dans les cas complexes et sensibles.

Pour en savoir plus

- [Recommandation CM/Rec\(2011\)12](#) du Comité des Ministres aux États membres sur les droits de l'enfant et les services sociaux adaptés aux enfants et aux familles .
- [Déclaration du Comité des Ministres sur les risques de la prise de décision assistée par ordinateur ou reposant sur l'intelligence artificielle dans le domaine du filet de sécurité sociale](#), 2021, en anglais uniquement.
- Conseil de l'Europe, [Children rights and social services, Report on the implementation of the Council of Europe Recommendation on children's rights and social services friendly to children and families](#), 2016, en anglais uniquement.
- Ivana Bartoletti et Raphaële Xenidis, Conseil de l'Europe, [Study on the impact of artificial intelligence systems, their potential for promoting equality, including gender equality, and the risks they may cause in relation to non-discrimination](#) (GEC/CDADI Study), 2023, en anglais uniquement.
- Commission de Venise, [The Netherlands – Opinion on the legal protection of citizens](#), CDL-AD(2021)031, 2021, en anglais uniquement.
- Conseil de l'Europe, [Social Security as a human right](#), Human Rights Files n° 23, 2007, en anglais uniquement.
- OECD Artificial Intelligence Papers, [AI and the future of social protection in OECD countries](#), n° 42, 2025, en anglais uniquement.
- Nations Unies, Rapporteur spécial sur les droits de l'homme et l'extrême pauvreté, [Rapport sur la privatisation des services publics](#), 26 septembre 2018.
- Rapporteur spécial sur les droits de l'homme et l'extrême pauvreté, [Rapport sur les États-providence numériques et les droits humains](#), A/74/493, 11 octobre 2019.
- Amnesty International, [Xenophobic Machines: Discrimination through unregulated use of algorithms in the Dutch childcare benefits scandal](#), 2021, en anglais uniquement.

4.7. L'éducation

188. Ce secteur comprend des activités liées à l'enseignement, l'accès à l'apprentissage, l'évaluation des élèves, l'orientation et la formation professionnelles, l'apprentissage tout au long de la vie et les résultats éducatifs.

Principaux cas d'utilisation de l'IA³⁴⁶

189. Dans le domaine de l'éducation, les systèmes d'IA sont utilisés pour améliorer l'apprentissage, soutenir les fonctions administratives et aider les enseignants grâce à l'analyse et à l'automatisation basées sur l'IA. Les cas d'utilisation sont les suivants :

- **Soutien à l'apprenant** : systèmes de tutorat pilotés par l'IA fournissant un enseignement personnalisé, outils d'apprentissage adaptatif s'ajustant aux progrès individuels et 'chatbots' offrant une assistance aux étudiants 24 heures sur 24 et 7 jours sur 7, y compris pour l'apprentissage tout au long de la vie.
- **Évaluation et retour d'information** : l'IA automatise l'évaluation des écrits, génère des analyses de performance en temps réel, utilise des modèles d'apprentissage ouverts pour aider les étudiants à suivre leurs progrès et aide à détecter le plagiat dans les travaux des étudiants en analysant les bases de données à la recherche de similitudes avec le contenu existant. La surveillance par l'IA évalue le comportement, l'environnement et les mouvements d'une personne qui passe un examen.
- **Administration de l'enseignement** : l'IA optimise les processus d'admission, automatise les emplois du temps et gère les systèmes d'apprentissage afin de rationaliser les opérations institutionnelles.
- **Soutien aux enseignants** : l'IA sélectionne des supports d'apprentissage à partir de sources en ligne et crée des contenus d'apprentissage adaptatifs et des manuels dynamiques. Elle fournit des analyses en temps réel en classe grâce à des tableaux de bord permettant d'analyser les données relatives aux performances, à l'assiduité, à la participation et à l'engagement des élèves, et aide à la planification des cours et à la gestion du temps.
- **Analyse de l'apprentissage et allocation des ressources** : l'IA analyse l'engagement des étudiants, prédit les résultats de

³⁴⁶ Artificial intelligence and education - A critical view through the lens of human rights, democracy and the rule of law (2022), pp.15-23 ; voir aussi UNESCO, Artificial Intelligence and Education : Guidance for Policy Makers (2021) , pp. 13-19

l'apprentissage et informe sur la distribution des ressources afin d'améliorer l'efficacité de l'enseignement.

- **Reconnaissance de la parole et traitement du langage** : les outils de reconnaissance vocale et de traitement du langage basés sur l'IA peuvent aider les étudiants handicapés en convertissant la parole en texte ou en fournissant une traduction et une transcription en temps réel.

Droits humains et principes pertinents

190. L'article 2 du protocole n° 1 de la CEDH garantit le droit à l'éducation, indispensable à la promotion des droits humains dans une société démocratique³⁴⁷. Il s'applique à l'enseignement préscolaire obligatoire³⁴⁸, à l'enseignement primaire et secondaire, ainsi qu'aux établissements d'enseignement supérieur créés par l'État³⁴⁹. Le droit à l'éducation peut donner lieu à des limitations implicitement acceptées, compte tenu du fait que le droit d'accès à l'éducation « appelle, par sa nature même, une réglementation de la part de l'État »³⁵⁰. Par conséquent, les autorités nationales jouissent d'une certaine marge d'appréciation., mais les restrictions ne doivent pas porter atteinte à l'essence du droit ou le rendre ineffectif ; elles doivent être prévisibles pour les intéressés et poursuivre un but légitime³⁵¹. Bien qu'il n'existe pas de liste exhaustive des « buts légitimes » qui peuvent être poursuivis en limitant la jouissance du droit à l'éducation³⁵², toute limitation doit maintenir un équilibre proportionné entre les moyens employés et le but recherché.³⁵³ L'État a des responsabilités concernant les écoles publiques et privées³⁵⁴.

191. L'article 2 du Protocole n° 1 doit être interprété en harmonie avec les autres règles du droit international dont la CEDH fait partie, notamment la Convention des Nations Unies relative aux droits de l'enfant, le Pacte

³⁴⁷ *Timishev c. Russie*, n°s 55762/2000 et 55974/00, 13 décembre 2005, paragraphe 64.

³⁴⁸ *Dieri & autres c. Lettonie*, n°s 50942/20 et 2022/21, 18 juillet 2024, paragraphes 118 et 122.

³⁴⁹ *Leyla Şahin c. Turquie* [GC], n° 44774/98, 10 novembre 2005, paragraphes 137 et 141.

³⁵⁰ *Affaire relative à certains aspects du régime linguistique de l'enseignement en Belgique (au principal)*, n°s 1474/62, 1677/62, 1691/62, 1769/63, 1994/63, 2126/64, 23 juillet 1968, paragraphe 5 de « La loi » partie I.A (affaire dite « linguistique belge »).

³⁵¹ *Leyla Şahin c. Turquie* [GC], n° 44774/98, 10 novembre 2005, paragraphe 154.

³⁵² Contrairement aux articles 8, 9, 10 et 11 de la CEDH.

³⁵³ *Leyla Şahin c. Turquie* [GC], n° 44774/98, 10 novembre 2005, paragraphes 154 et suivants.

³⁵⁴ *Kjeldsen, Busk Madsen et Pedersen c. Danemark*, n°s 5095/71, 5920/72 et 5926/72, 7 décembre 1976. Voir également *O'Keefe c. Irlande* [GC], n° 35810/09, 28 janvier 2014, paragraphes 144-152.

international relatif aux droits économiques, sociaux et culturels, la Convention internationale sur l'élimination de toutes les formes de discrimination raciale, la Convention de l'UNESCO concernant la lutte contre la discrimination dans le domaine de l'enseignement³⁵⁵, la Convention des Nations Unies relative aux droits des personnes en situation de handicap³⁵⁶ et la CSE³⁵⁷. Les États doivent respecter et remplir les obligations et les engagements prévus par les normes existantes du Conseil de l'Europe et des Nations unies en matière de droits de l'enfant.

192. En ce qui concerne la CSE (Révisée), les États parties sont tenus, en vertu de la partie II, article 17 paragraphe 2, soit directement, soit en partenariat avec des organisations publiques et privées, de mettre en œuvre des mesures qui assurent un enseignement primaire et secondaire gratuit à tous les individus de moins de 18 ans (à moins que la majorité ne soit atteinte plus tôt en vertu de la loi applicable à l'enfant)³⁵⁸. L'article 17 exige des États parties qu'ils mettent en place et maintiennent un système éducatif qui soit à la fois accessible et efficace³⁵⁹. Si les acteurs privés peuvent apporter leur contribution, leur participation ne doit pas nuire à la qualité ou à l'accessibilité de l'enseignement public³⁶⁰. Les États parties doivent assurer une formation professionnelle efficace en promouvant des programmes techniques et professionnels pour tous³⁶¹. En vertu de l'article 17, l'égalité des chances en matière d'éducation doit être garantie pour tous les enfants, en particulier pour les groupes à risque³⁶².

Droit à la vie privée et à la protection des données

193. L'utilisation de systèmes d'IA à des fins éducatives peut conduire au traitement de données à caractère personnel, par exemple, d'enfants, d'étudiants universitaires, de personnes en situation de handicap, de personnes en formation professionnelle, d'apprenants tout au long de la

³⁵⁵ *Catan et autres c. République de Moldova et Russie [GC]*, nos 43370/04, 8252/05 et 18454/06), 19 octobre 2012, paragraphe 136

³⁵⁶ *Çam c. Turquie*, n° 51500/08, 23 février 2016, paragraphe 53

³⁵⁷ voir *Ponomaryovi c. Bulgarie*, n° 5335/05, 21 juin 2011, paragraphes 34-35, se référant à la Charte sociale européenne révisée.

³⁵⁸ Sans préjudice d'autres dispositions spécifiques prévues par la CSE, notamment l'article 7. Voir l'annexe à la Charte sociale européenne (révisée) - Série des traités européens – n° 163.

³⁵⁹ *Conclusions 2003*, Bulgarie, Comité européen des droits sociaux.

³⁶⁰ *Conclusions 2019, Déclaration d'interprétation sur l'article 17* paragraphe 2 - *Participation du secteur privé à l'éducation*, Comité européen des droits sociaux.

³⁶¹ *Conclusions I (1969), Déclaration d'interprétation de l'article 10* paragraphe 1, Comité européen des droits sociaux.

³⁶² *Mental Disability Advocacy Center (MDAC) c. Bulgarie*, réclamation n° 41/2007, décision sur le bien-fondé du 3 juin 2008, paragraphe 34, citant les *Conclusions 2003*, Bulgarie.

vie, d'éducateurs ou de parents par divers acteurs, notamment les gouvernements nationaux, les établissements d'enseignement publics et privés, les entreprises commerciales telles que les fournisseurs de produits ou de services, les développeurs de logiciels et les particuliers tels que les enseignants, les tuteurs légaux et les camarades de classe. Le traitement des données à caractère personnel d'un enfant dans le cadre éducatif est particulièrement complexe en raison du contexte non-consensuel dans lequel il s'inscrit, ce qui peut avoir une incidence sur la nature librement consentie du consentement. En particulier, en règle générale, les enfants ne peuvent pas conclure de contrats³⁶³. L'utilisation de systèmes d'intelligence artificielle dans le contexte éducatif doit donc être examinée au regard de l'article 8 de la CEDH.

194. Le document [CM/Rec\(2018\)7](#), qui fournit des "Lignes directrices relatives au respect, à la protection et à la réalisation des droits de l'enfant dans l'environnement numérique", reconnaît que les données à caractère personnel peuvent être traitées au profit des enfants, mais souligne que les États devraient prendre des mesures pour veiller à ce que les données à caractère personnel des enfants soient traitées de manière loyale, licite, précise et sécurisée, à des fins spécifiques et avec le consentement libre, explicite, éclairé et univoque des enfants et/ou de leurs parents, soignants ou représentants légaux, ou conformément à une autre base légitime prévue par la loi. Le principe de minimisation des données doit être respecté, ce qui signifie que le traitement des données à caractère personnel doit être adéquat, pertinent et non excessif au regard des finalités pour lesquelles elles sont traitées.³⁶⁴

195. Les États devraient veiller à ce que le traitement de catégories particulières de données, considérées comme sensibles, ne soit autorisé dans tous les cas que lorsque des garanties appropriées sont inscrites dans la loi. Le profilage des enfants, c'est-à-dire toute forme de traitement automatisé de données à caractère personnel consistant à appliquer un « profil » à un enfant, notamment pour prendre des décisions le concernant ou pour analyser ou prédire ses préférences personnelles, son comportement et ses attitudes, devrait être interdit par la loi. Dans des circonstances exceptionnelles, les États peuvent lever cette restriction lorsque cela est dans l'intérêt supérieur de l'enfant ou s'il existe un intérêt public supérieur, à condition que des garanties appropriées soient prévues par la loi. Le profilage doit également être exclu en ce qui concerne les jeunes et les adultes dans les contextes éducatifs. Les outils éducatifs basés sur des systèmes d'IA, tels que l'analyse en temps réel des salles

³⁶³ Artificial intelligence and education - A critical view through the lens of human rights, democracy and the rule of law (2022), p. 71, Conseil de l'Europe (*en anglais uniquement*).

³⁶⁴ Lignes directrices sur la protection des données personnelles des enfants dans un cadre exécutif, Comité consultatif de la Convention 108 (T-PD)

de classe et le suivi de l'engagement des étudiants ou l'IA de contrôle qui surveille les étudiants par reconnaissance faciale et suivi comportemental, peuvent interférer avec le droit au respect de la vie privée. Cette préoccupation ne concerne pas seulement les enfants, mais aussi les étudiants adultes et le personnel éducatif soumis à une surveillance ou à une évaluation des performances au moyen de technologies similaires. Les personnes ne doivent pas être soumises à des ingérences arbitraires ou illégales dans leur vie privée. Toute ingérence doit être conforme à la loi, poursuivre un objectif légitime, être nécessaire dans une société démocratique et être proportionnée à l'objectif légitime poursuivi. Les mesures de surveillance ou d'interception, en particulier, doivent respecter ces conditions et faire l'objet d'un contrôle efficace, indépendant et impartial³⁶⁵.

Non-discrimination et égalité

196. Le droit à l'éducation prévu à l'article 2 du Protocole n° 1 à la CEDH, lu conjointement avec l'article 14 de la CEDH, exige que les États traitent les risques liés à la non-discrimination et à l'égalité pour tous les individus dans le contexte éducatif³⁶⁶. Dans le contexte des systèmes d'IA, cela implique de veiller à ce que les systèmes d'IA ne renforcent pas les préjugés susceptibles d'entraîner des résultats discriminatoires ou de créer des obstacles à l'accès à l'éducation, ou des inégalités dans le niveau et la qualité de l'éducation. Les enfants, en particulier, et en raison de leur stade de développement, ont des besoins et des droits spécifiques qui les distinguent des adultes. Il est donc nécessaire de mettre en place des réglementations axées sur les enfants dans le cadre de l'acquisition et de l'utilisation des technologies éducatives, y compris les systèmes d'intelligence artificielle³⁶⁷. Dans toutes les actions concernant les enfants, qu'elles soient entreprises par des institutions publiques ou privées de protection sociale, des tribunaux, des autorités administratives ou des organes législatifs, l'intérêt supérieur de l'enfant doit être une considération primordiale³⁶⁸.

³⁶⁵ CM/Rec(2018)7 Lignes directrices relatives au respect, à la protection et à la réalisation des droits de l'enfant dans l'environnement numérique

³⁶⁶ Plusieurs traités internationaux interdisent la discrimination dans l'éducation, notamment la Convention de l'UNESCO de 1960 contre la discrimination dans l'enseignement, le Pacte international relatif aux droits économiques, sociaux et culturels de 1966 (article 13), la Convention des Nations unies relative aux droits de l'enfant de 1989 (article 28) et la Convention relative aux droits des personnes en situation de handicap (article 24).

³⁶⁷ Preparatory study for the development of a legal instrument on regulating the use of artificial intelligence systems in education, Revised draft (mars 2024) (*en anglais uniquement*), Unité de transformation numérique du département de l'éducation, Conseil de l'Europe.

³⁶⁸ Convention des Nations Unies relative aux droits de l'enfant (1989), article 3. Pour « l'intérêt supérieur de l'enfant », voir Neulinger et Shuruk [GC], n° 41615/07, 6 juillet

197. Compte tenu de l'importance croissante des nouvelles technologies, plusieurs documents du Conseil de l'Europe ont été adoptés dans ce domaine, invitant les États à veiller à ce que les enfants aient un accès à l'environnement numérique de manière non discriminatoire et inclusive, en tenant compte des capacités en développement des enfants et des circonstances particulières des enfants en situation de vulnérabilité³⁶⁹. Cela devrait également s'appliquer dans les situations où des systèmes d'IA sont impliqués. Des efforts doivent être entrepris pour respecter, protéger et réaliser les droits de chaque enfant dans un cadre éducatif, mais des mesures ciblées peuvent être nécessaires pour répondre aux besoins spécifiques, en reconnaissant que les systèmes d'IA ont le potentiel à la fois d'augmenter la vulnérabilité des enfants et de les autonomiser, protéger et soutenir.³⁷⁰

198. Dans le contexte de l'article 14 de la CEDH, les obligations positives des États pourraient inclure des mesures visant à corriger les « inégalités de fait »³⁷¹. L'action positive, ou les mesures temporaires spéciales, peuvent comprendre des mesures visant à prévenir ou à compenser les désavantages subis par les groupes exposés à la discrimination et à l'intolérance et à faciliter leur pleine participation dans tous les domaines de la vie³⁷². Les États membres devraient ainsi veiller à ce que les établissements d'enseignement utilisent les systèmes d'IA de manière inclusive³⁷³. Les États devraient également s'efforcer de renforcer l'utilisation des technologies de l'information et de la communication par les filles et de promouvoir l'égalité des chances et des résultats pour tous les enfants³⁷⁴. En outre, des systèmes tels que la reconnaissance faciale, utilisée dans le cadre d'un système d'IA de surveillance conçu pour contrôler le comportement des étudiants pendant les examens en ligne,

2010, paragraphes 49-56. La Cour place également au premier plan « l'intérêt supérieur de l'enfant », qui peut, selon sa nature et sa gravité, prévaloir sur celui des parents (ibid., paragraphe 134).

³⁶⁹ CM/Rec(2018)7 Lignes directrices relatives au respect, à la protection et à la réalisation des droits de l'enfant dans l'environnement numérique, 4 juillet 2018.

³⁷⁰ Lignes directrices du Conseil de l'Europe sur la protection des données des enfants dans un cadre éducatif (2020), Comité sur la Convention 108, T-PD(2019)06BISrev5, paragraphe 5.4

³⁷¹ *Guide sur l'article 14 de la Convention européenne des droits de l'homme et sur l'article 1 du Protocole 12*, CEDH, p. 14.

³⁷² Voir également la Recommandation de politique générale n° 2 révisée de l'ECRI sur les organismes de promotion de l'égalité chargés de lutter contre le racisme et l'intolérance au niveau national, paragraphe 60, et la Recommandation de politique générale n° 7 révisée de l'ECRI sur la législation nationale pour lutter contre le racisme et la discrimination raciale, paragraphe 5.

³⁷³ Recommandation CM/Rec(2019)1 sur la prévention et la lutte contre le sexisme, en particulier II.G. « Établissements d'enseignement ».

³⁷⁴ CM/Rec(2018)7 Lignes directrices relatives au respect, à la protection et à la réalisation des droits de l'enfant dans l'environnement numérique, 4 juillet 2018, paragraphe 46

peuvent présenter des préjugés et conduire à une discrimination intersectionnelle, notamment fondée sur la race et le sexe³⁷⁵. En vertu de la CEDH, toute différence de traitement doit poursuivre un but légitime et être proportionnée³⁷⁶. Il convient donc d'accorder une attention particulière à l'utilisation des systèmes d'IA dans les procédures de sélection et d'examen, afin d'éviter les résultats discriminatoires.

199. En outre, un accès limité aux systèmes et outils d'IA peut empêcher les individus ou les groupes de bénéficier de leurs avantages, entraînant ainsi des désavantages dans divers secteurs, notamment l'éducation. La littératie en IA, qui pourrait être considérée comme une extension ou une spécialisation de la littératie numérique, devrait être incluse dans le programme d'éducation de base dès les premières années, en tenant compte des capacités en développement des enfants.³⁷⁷ Cela comprend les compétences techniques, les compétences en matière de création de contenu et la compréhension critique des risques et des opportunités en ligne. Les efforts devraient se concentrer sur les écoles, les organisations centrées sur les enfants et les parents ou tuteurs, afin de garantir un environnement numérique sûr et inclusif. Les politiques d'éducation numérique ne devraient pas désavantager les enfants qui manquent de ressources à la maison ou qui vivent dans des institutions. Un soutien particulier devrait être apporté aux enfants ayant un accès limité ou inexistant au numérique, y compris ceux issus de milieux socio-économiquement défavorisés et les enfants en situation de handicap. Les États devraient également œuvrer pour combler la fracture numérique et l'écart entre les sexes dans le domaine des technologies, en garantissant des chances égales pour tous les enfants, quels que soient leur origine, avec une attention particulière portée aux filles, afin qu'elles puissent accéder aux outils numériques, y compris les systèmes d'IA, et en tirer parti.³⁷⁸

³⁷⁵ Étude CDADI/GEC (2023), p. 24.

³⁷⁶ Par exemple, les modifications d'un système d'accès à l'université qui ont conduit à une différence de traitement ont emporté violation de l'article 14, combiné avec l'article 2 du Protocole n° 1, alors qu'elles visaient à améliorer rapidement la qualité de l'enseignement supérieur. L'application imprévisible du nouveau système, conjuguée à l'absence de mesures correctives, a rendu sa mise en œuvre disproportionnée par rapport à ce but - voir *Altınay c. Turquie*, n° 37222/04, 9 juillet 2013, paragraphe 60.

³⁷⁷ Recommandation CM/Rec(2019)10 visant à développer et à promouvoir l'éducation à la citoyenneté numérique, 21 novembre 2019 ; Recommandation CM/Rec(2016)2 sur l'Internet des citoyens, 10 février 2016.

³⁷⁸ CM/Rec(2018)7 Lignes directrices relatives au respect, à la protection et à la réalisation des droits de l'enfant dans l'environnement numérique, 4 juillet 2018, paragraphes 41-46.

Transparence et responsabilité

200. Le manque de transparence, d'explicabilité et d'interprétabilité des systèmes d'IA (le « problème de la boîte noire ») présente des risques dans le contexte de l'éducation. Si un système d'IA fait des recommandations sur le parcours d'apprentissage d'un enfant ou fournit des recommandations qui peuvent avoir des conséquences à long terme sur le développement de l'enfant, les enseignants et les parents doivent être en mesure de comprendre le raisonnement qui sous-tend ses décisions, y compris les paramètres utilisés, et avoir la possibilité de les évaluer et de les annuler si nécessaire. De même, les systèmes d'IA utilisés pour les admissions ou les examens pourraient avoir des conséquences importantes sur les possibilités d'éducation et les perspectives d'avenir des titulaires de droits. L'opacité de l'IA peut également rendre difficile l'obtention d'un consentement véritablement éclairé ou la contestation de ses décisions et résultats³⁷⁹. Le consentement doit être donné librement sans ambiguïté et pouvoir être refusé sans préjudice³⁸⁰. Des niveaux de transparence suffisants doivent être garantis. Il en va de même pour les apprenants adultes.

201. Les États membres devraient également veiller à la mise en œuvre effective de leurs au titre de l'article 13 de la CEDH afin de garantir le droit des enfants et des apprenants adultes à un recours effectif lorsque leurs droits humains et leurs libertés fondamentales ont été violés par l'utilisation de systèmes d'intelligence artificielle dans le contexte éducatif.

202. En particulier pour les enfants, cela implique la mise à disposition de moyens disponibles, connus, accessibles, abordables et adaptés aux enfants, par lesquels les enfants, ainsi que leurs parents ou représentants légaux, peuvent déposer des plaintes et demander réparation. Les recours effectifs peuvent comprendre, en fonction de la violation en question, une enquête, une explication, une réponse, une correction, une procédure, le retrait immédiat du contenu illicite, des excuses, une réintégration, une reconnexion et une indemnisation³⁸¹. Les États devraient également veiller à ce que, dans tous les cas, l'accès aux tribunaux ou le contrôle judiciaire des recours administratifs et autres procédures soient disponibles, conformément aux principes énoncés dans les [Lignes directrices du Comité des Ministres du Conseil de l'Europe sur une justice adaptée aux enfants](#) (2010).

³⁷⁹ Ibid, p. 52.

³⁸⁰ Lignes directrices sur la protection des données personnelles des enfants dans un cadre éducatif (2020), Comité du Conseil de l'Europe sur la Convention 108, T-PD(2019)06BISrev5.

³⁸¹ CM/Rec(2018)7, paragraphe 67.

Entreprises et droits humains

203. Le rôle du secteur privé dans l'éducation prend de plus en plus d'importance, que ce soit par le biais des écoles privées ou par l'acquisition auprès d'entreprises privées de systèmes d'enseignement et de gestion scolaire basés sur l'IA destinés à être utilisés dans les écoles publiques. Les États doivent veiller à ce que les entreprises et autres partenaires clés assument leurs responsabilités en matière de droits humains et soient tenus de rendre des comptes en cas d'abus. Les entreprises ont la responsabilité de respecter les droits humains, y compris les droits de l'enfant, comme l'affirment les Principes directeurs relatifs aux entreprises et aux droits de l'homme des Nations unies et la Recommandation [CM/Rec\(2016\)3](#) du Comité des ministres aux États membres sur les droits de l'homme et les entreprises³⁸². En vertu de la CEDH, les États ne peuvent s'exonérer de leur responsabilité en déléguant leurs obligations à des organismes privés ou à des particuliers. Cela inclut l'enseignement dispensé par les écoles privées et leur personnel, dont les actes peuvent engager la responsabilité de l'État³⁸³.

204. La Recommandation [CM/Rec\(2018\)7](#) du Comité des ministres recommande aux États d'exiger des entreprises commerciales et des autres parties prenantes concernées qu'elles s'acquittent de leur responsabilité de respecter les droits de l'enfant dans l'environnement numérique et de les encourager à soutenir et à promouvoir ces droits. Les États devraient promouvoir et inciter les entreprises commerciales à mettre en œuvre la sécurité dès la conception, la protection de la vie privée dès la conception et la protection de la vie privée par défaut en tant que principes directeurs pour les caractéristiques et fonctionnalités des produits et services adressés aux enfants ou utilisés par eux.

205. Les États devraient prendre des mesures appropriées pour protéger les enfants contre les violations des droits humains commises par les entreprises dans l'environnement numérique et pour veiller à ce que les enfants aient accès à un recours effectif. Il s'agit notamment de mettre en œuvre des politiques et des mesures visant à encourager les entreprises à mettre en place leurs propres mécanismes de recours et de réclamation, conformément aux critères d'efficacité définis dans les principes directeurs des Nations unies, tout en veillant à ce que ces mécanismes n'entravent pas l'accès de l'enfant aux mécanismes judiciaires ou non judiciaires de l'État. Les États devraient également encourager les entreprises à fournir des informations accessibles, adaptées à l'âge et disponibles dans la langue de l'enfant sur la manière de déposer des plaintes et de demander réparation par le biais de

³⁸² Voir section VI.

³⁸³ *Costello-Roberts c. Royaume-Uni*, n° 13134/87, 25 mars 1993, paragraphe 27.

mécanismes de recours et de réclamation. En outre, les entreprises commerciales devraient être tenues de mettre à disposition, sur leur plateforme ou au sein de leur service, des moyens facilement accessibles permettant à toute personne, et en particulier aux enfants, de signaler tout matériel ou activité qui les inquiète, en veillant à ce que les signalements reçus soient traités de manière efficace et dans des délais raisonnables³⁸⁴. Il devrait y avoir des moyens accessibles et efficaces de signaler les préjugés, les erreurs ou les préoccupations concernant les systèmes éducatifs pilotés par l'IA qui pourraient avoir un impact sur les titulaires de droits.

Pour en savoir plus

- CEDH, [Guide sur l'article 2 du Protocole n° 1 - Droit à l'instruction](#)
- Conseil de l'Europe, [Réglementer l'utilisation des systèmes d'IA dans l'éducation](#), 2024, en anglais uniquement
- Conseil de l'Europe, [The state of artificial intelligence and education across Europe – Results of a survey of Council of Europe member states \(2024\)](#), 2024, en anglais uniquement
- Conseil de l'Europe, [1st Working Conference "Artificial Intelligence and education: A critical view through the lens of human rights, democracy and the rule of law" - Conference highlights](#), 2022, en anglais uniquement
- Conseil de l'Europe, [Artificial intelligence and education - A critical view through the lens of human rights, democracy and the rule of law](#), 2022, en anglais uniquement
- Conseil de l'Europe, [2nd Working Conference "Artificial Intelligence and education: Regulating the use of AI in education" - Conference Report](#), 2024
- The Alan Turing Institute, [Mapping Study on the Rights of the Child and Artificial Intelligence – Legal Frameworks that Address AI in the Context of Children's Rights](#), approuvé par le Comité Directeur pour les Droits de l'Enfant (CDENF), 2024, en anglais uniquement
- Ilkka TUOMI, [Regulating artificial intelligence in the education domain: a general approach](#), 2024, en anglais uniquement
- Beth HAVINGA, [Towards a European review framework for AI EdTech systems](#), 2024, en anglais uniquement
- UNESCO, [Beijing Consensus on Artificial Intelligence and Education](#), 2019, en anglais uniquement
- UNESCO, [Artificial Intelligence and Education: Guidance for Policy Makers](#), 2021, en anglais uniquement
- Comité des droits de l'enfant de l'ONU, [General Comment n° 25 \(2021\) on children's rights in relation to the digital environment](#), en anglais uniquement

³⁸⁴ CM/Rec(2018)7, paragraphe 71.

- OECD, [Recommendation of the Council on Children in the Digital Environment](#), en anglais uniquement

4.8. Travail et emploi

206. Ce secteur comprend les activités liées à l'emploi, aux ressources humaines et à la gestion du travail, y compris, mais sans s'y limiter, des questions telles que le recrutement, l'accès à l'emploi, la gestion des performances et les politiques relatives aux travailleurs.

Principaux cas d'utilisation de l'IA

207. Sur le lieu de travail, les systèmes d'IA sont utilisés pour automatiser ou faciliter les décisions des ressources humaines en matière de recrutement et d'évaluation des candidats, pour automatiser des tâches traditionnellement effectuées par des travailleurs et pour soutenir les fonctions managériales par le biais d'analyses et d'algorithmes pilotés par l'IA - ce que l'on appelle communément la « gestion algorithmique ». Il s'agit notamment de :

- **Recrutement et embauche** : l'IA est utilisée pour créer des descriptions de poste optimisées et les diffuser sur les réseaux sociaux et les plateformes d'emploi, pour mettre en relation les offres d'emploi et les demandeurs d'emploi, pour automatiser la présélection des CV, la notation des candidats et les évaluations prédictives, ainsi que pour mener les premiers entretiens via des 'chatbots' ou des outils vidéo automatisés.
- **Automatisation des tâches et productivité** : les systèmes d'IA sont utilisés par les travailleurs pour automatiser des tâches routinières telles que la saisie ou la recherche de données, ainsi que des tâches non routinières telles que la création de textes, d'images ou de vidéos.
- **Gestion algorithmique** : l'IA optimise la planification, surveille la productivité et améliore l'automatisation des flux de travail ; les systèmes d'IA sont utilisés pour suivre et analyser les performances des employés, en utilisant les données pour identifier leurs points forts, leurs points faibles et les domaines susceptibles d'être améliorés.
- **Bien-être des employés** : les outils basés sur l'IA analysent le moral au travail, la satisfaction et l'engagement des employés, détectent les risques d'épuisement professionnel et personnalisent les programmes de soutien aux employés.

Droits humains et principes pertinents

208. La CEDH a été interprétée à travers le droit au respect de la vie privée (article 8 de la CEDH), la non-discrimination (article 14 et protocole n° 12 de la CEDH), la liberté d'expression (article 10 de la CEDH) et la liberté d'association (article 11 de la CEDH) pour englober certains droits liés au travail et à l'emploi tels que le droit à la négociation collective³⁸⁵ ou le droit de grève³⁸⁶ et pour reconnaître la valeur particulière de certains droits au travail tels que la protection de la vie privée sur le lieu de travail³⁸⁷ ou la santé au travail³⁸⁸. La CSE comprend un large éventail de droits du travail, tant individuels que collectifs³⁸⁹.

209. L'utilisation des systèmes d'IA peut avoir des conséquences considérables sur le travail et l'emploi, couvrant de nombreuses catégories de professions (y compris celles qui ont été relativement protégées des vagues précédentes d'automatisation), d'employeurs et de travailleurs. L'utilisation de systèmes d'IA pourrait entraver l'accès au travail, augmenter l'intensité du travail, renforcer ou exacerber les déséquilibres de pouvoir entre employeurs et travailleurs, réduire l'implication humaine dans les décisions d'embauche, d'évaluation et de licenciement, et porter atteinte aux principes fondamentaux et aux droits au travail. Les défis liés à l'IA sont particulièrement présents dans les nouvelles formes d'emploi telles que les plateformes ou le « gig work », une forme de travail temporaire³⁹⁰.

³⁸⁵ *Demir et Baykara c. Turquie*, n° 34503/97, 12 novembre 2008.

³⁸⁶ *Ognevenko c. Russie*, n° 44873/09, 20 novembre 2018, paragraphe 73.

³⁸⁷ *López Ribalda et autres c. Espagne* [GC], nos 1874/13 et 8567/13, 17 novembre 2019.

³⁸⁸ *Meier c. Suisse*, n° 10109/14, 9 février 2016.

³⁸⁹ Le droit de travailler, le droit à des conditions de travail justes, à des conditions de travail sûres et saines, à une rémunération équitable, à l'égalité des chances et à l'égalité de traitement en matière d'emploi et de profession sans discrimination fondée sur le sexe, le droit à la protection en cas de licenciement et à la protection des droits des travailleurs en cas d'insolvabilité de leur employeur, à la dignité au travail, le droit des travailleurs ayant des responsabilités familiales à l'égalité des chances et à l'égalité de traitement ; et le droit collectif : le droit de s'organiser et de négocier collectivement, le droit à l'information et à la consultation - également dans les procédures de licenciement collectif - et de participer à la détermination et à l'amélioration des conditions de travail et de l'environnement de travail, la protection des représentants des travailleurs dans l'entreprise et les facilités qui doivent leur être accordées.

³⁹⁰ Le travail via une plateforme est une forme d'emploi dans laquelle des organisations ou des individus utilisent une plateforme en ligne pour accéder à d'autres organisations ou individus afin de résoudre des problèmes spécifiques ou de fournir des services spécifiques en échange d'un paiement. L'économie des plateformes numériques (ou « gig economy ») s'est développée de manière exponentielle pendant et après la pandémie de Covid-19.

Droit à la vie privée et à la protection des données

210. L'article 8 protège le droit au respect de la vie privée sur le lieu de travail, ce qui englobe la confidentialité de la correspondance³⁹¹, l'utilisation du courrier électronique³⁹², la protection des données³⁹³, l'accès aux données³⁹⁴, la réputation professionnelle³⁹⁵, et fournit des motifs de protection en cas de licenciements abusifs³⁹⁶.

211. Les États peuvent également être tenus d'adopter des mesures visant à garantir le respect de la vie privée, même dans le domaine des relations entre les individus, en tenant compte de l'équilibre équitable qui doit être trouvé entre des intérêts concurrents³⁹⁷. Compte tenu du fait que le droit du travail laisse aux parties à un contrat de travail la possibilité de négocier le contenu de leurs relations, les États disposent d'une large marge d'appréciation pour évaluer la nécessité d'établir un cadre juridique régissant les conditions dans lesquelles un employeur peut réglementer les communications électroniques ou autres de nature non professionnelle de ses employés sur le lieu de travail³⁹⁸. Toutefois, les autorités nationales devraient veiller à ce que l'introduction par un employeur de mesures de surveillance de la correspondance et d'autres communications, quelles que soient l'étendue et la durée de ces mesures, s'accompagne de garanties adéquates et suffisantes contre les abus³⁹⁹. À la lumière des développements rapides dans ce domaine, des facteurs pertinents ont été identifiés pour la proportionnalité, ainsi que des garanties procédurales contre l'arbitraire⁴⁰⁰. Les autorités nationales devraient veiller à ce qu'un employé dont les communications ont été surveillées ait accès à un recours devant une instance judiciaire⁴⁰¹.

³⁹¹ *Bărbulescu c. Roumanie* [GC], n° 61496/08, 5 septembre 2011.

³⁹² *Copland c. Royaume-Uni*, n° 62617/00, 3 avril 2007.

³⁹³ *Surikov c. Ukraine*, n° 42788/06, 26 janvier 2017.

³⁹⁴ *Yonchev c. Bulgarie*, n° 12504/09, 7 décembre 2017.

³⁹⁵ *S.W. c. Royaume-Uni*, n° 87/18, 22 juin 2021.

³⁹⁶ *Ülya Ebru Demirel c. Turquie*, n° 30733/08, 19 juin 2018 ; *Denisov c. Ukraine* [GC], n° 76639/11, 25 septembre 2018.

³⁹⁷ *Köpke c. Allemagne (déc.)*, n° 420/07, 5 octobre 2010, avec d'autres références.

³⁹⁸ *Barbulescu c. Roumanie* [GC], paragraphe 118-119.

³⁹⁹ Ibid. paragraphe 120.

⁴⁰⁰ Ibid. paragraphe 121. Les facteurs pertinents sont les suivants (i) si l'employé a été clairement informé à l'avance de la surveillance ; (ii) l'étendue et le caractère intrusif de la surveillance ; (iii) si l'employeur avait des raisons légitimes de surveiller les communications, en particulier d'accéder à leur contenu ; (iv) s'il existait des solutions moins intrusives ; (v) les conséquences pour l'employé et la manière dont les résultats de la surveillance ont été utilisés ; et (vi) si des garanties adéquates ont été mises en place pour protéger la vie privée de l'employé.

⁴⁰¹ Ibid. paragraphe 122.

212. En ce qui concerne la légalité, les politiques des employeurs peuvent être suffisantes dans les cas où les questions relatives au marché du travail sont, selon le cadre juridique de l'État, principalement réglementées par les parties prenantes du marché du travail et permettent à l'employeur d'exercer son droit de gérer et d'organiser le travail⁴⁰². Pour qu'il en soit ainsi, dans les cas concernant les obligations positives de l'État en vertu de l'article 8, le droit à la vie privée de l'individu doit être effectivement protégé et correctement mis en balance avec les droits de l'employeur par les tribunaux nationaux. Il s'agit notamment des cas de licenciement d'employés pour non-respect de leurs obligations, révélés par la vidéosurveillance, de la surveillance par⁴⁰³ des messages privés envoyés à partir d'un compte de messagerie d'entreprise⁴⁰⁴, et de l'accès de l'employeur aux fichiers des employés sur un ordinateur⁴⁰⁵.

213. Pour la CSE, le droit de travailler librement inclut la protection contre les intrusions injustifiées dans la vie privée (article 1, paragraphe 2)⁴⁰⁶. L'ingérence dans la vie privée peut prendre diverses formes, notamment la collecte de données par l'employeur (par le biais de la vidéosurveillance⁴⁰⁷ ou de la vérification des courriels des employés⁴⁰⁸), leur stockage, leur partage et leur utilisation pour prendre des décisions en matière d'emploi. Les employés doivent être protégés contre de telles ingérences, en particulier lorsqu'elles se produisent par le biais de la communication électronique et du traitement des données⁴⁰⁹. Les articles 1 paragraphes 2 et 26 (protection contre le harcèlement) protègent globalement contre les intrusions inutiles sur le lieu de travail, mais les violations de la vie privée des salariés peuvent également enfreindre l'article 3 (santé des travailleurs, y compris santé mentale), l'article 5 (affiliation syndicale), l'article 6 (négociation collective), l'article 11 (santé mentale), l'article 20 (discrimination fondée sur le sexe) et l'article 24 (licenciement injustifié)⁴¹⁰. La question de la vie privée au travail peut également être réglementée par des conventions collectives⁴¹¹. En outre, l'article 3 (droit à un lieu de travail sûr et sain) s'applique aux secteurs public et privé, tant aux salariés qu'aux indépendants⁴¹². En ce qui concerne l'application de ce droit, l'introduction de nouvelles technologies

⁴⁰² *Wretlund c. Suède*, n° 46210/99, décision du 9 mars 2004 (irrecevable).

⁴⁰³ *Köpke c. Allemagne*, n° 420/07, décision du 5 octobre 2010 (irrecevable) ; *López Ribalda et autres c. Espagne* [GC], n° 1874/13 et 8567/13, 17 octobre 2019.

⁴⁰⁴ *Barbulescu c. Roumanie* [GC].

⁴⁰⁵ *Libert c. France*, n° 588/13, 22 février 2018.

⁴⁰⁶ Conclusions 2012, Déclaration d'interprétation de l'article 1 paragraphe 2.

⁴⁰⁷ Conclusions 2020, Géorgie.

⁴⁰⁸ Conclusions XXI-1, Islande.

⁴⁰⁹ Conclusions 2012, Déclaration d'interprétation de l'article 1 paragraphe 2.

⁴¹⁰ Conclusions 2012, Déclaration d'interprétation de l'article 1 paragraphe 2.

⁴¹¹ Conclusions 2016, Belgique.

⁴¹² Conclusions II (1971), Déclaration d'interprétation de l'article 3 ; Conclusions 2013, Déclaration d'interprétation de l'article 3 paragraphe 3.

peut générer, accroître et déplacer des facteurs de risque pour la santé et la sécurité des travailleurs. En particulier, les nouvelles technologies, les contraintes organisationnelles et les exigences psychologiques favorisent le développement de facteurs de risque psychosociaux, conduisant au stress, à l'agression, à la violence et au harcèlement liés au travail⁴¹³. Les États parties à la CSE (ou à la Charte sociale européenne révisée) doivent revoir la prévention des risques professionnels au niveau national et au niveau de l'entreprise, en consultation avec les partenaires sociaux (article 3, paragraphe 1)⁴¹⁴. En vertu de l'article 3 paragraphe 2, ils devraient adopter des réglementations en matière de santé et de sécurité alignées sur les normes scientifiques et internationales,⁴¹⁵ en veillant à ce que les responsabilités de l'employeur et les droits et devoirs du travailleur soient clairement définis.

Non-discrimination et égalité

214. L'article 14 et le protocole n° 12 de la CEDH interdisent la discrimination dans le domaine de l'emploi pour un large éventail de motifs. La discrimination fondée sur le sexe dans le domaine de l'emploi est un problème récurrent : « lorsqu'une différence de traitement est fondée sur le sexe, la marge d'appréciation accordée à l'État est étroite et, dans de telles situations, le principe de proportionnalité n'exige pas seulement que la mesure choisie soit en général adaptée à la réalisation de l'objectif poursuivi, mais il doit également être démontré qu'elle était nécessaire dans les circonstances »⁴¹⁶. La promotion de l'égalité de genre est aujourd'hui un objectif majeur dans les États membres du Conseil de l'Europe et des raisons très sérieuses devraient être avancées pour qu'une telle différence de traitement puisse être considérée comme compatible avec la CEDH⁴¹⁷.

215. En ce qui concerne le CES, afin de respecter pleinement les droits à l'accès à l'emploi (article 1 paragraphe 2)⁴¹⁸, à l'égalité de rémunération entre les genres (article 4 paragraphe 3)⁴¹⁹, et à l'accès à l'égalité des

⁴¹³ Conclusions 2013, Déclaration d'interprétation sur l'article 3.

⁴¹⁴ Conclusions 2003, Déclaration d'interprétation sur l'article 3 paragraphe 1 ; voir en particulier Conclusions 2003, Bulgarie ; Déclaration sur la Covid-19 et les droits sociaux adoptée le 24 mars 2021.

⁴¹⁵ *Fondation Marangopoulos pour les droits de l'homme (FMDH) c. Grèce*, réclamation n° 30/2005, décision sur le bien-fondé du 6 décembre 2006, paragraphe 224.

⁴¹⁶ *Emel Boyraz c. Turquie*, n° 61960/08, 2 décembre 2014, paragraphe 51 (*en anglais uniquement, traduction libre*).

⁴¹⁷ Ibid.

⁴¹⁸ Conclusions XVI-1 (2003), Islande.

⁴¹⁹ *University Women of Europe (UWE) c. Belgique*, plainte n° 124/2016, décision sur le fond du 6 décembre 2019, paragraphe 115.

chances en matière d'emploi (article 20)⁴²⁰, les États parties doivent mettre en œuvre des mesures juridiques garantissant l'application effective de l'interdiction de la discrimination. En cas de plainte pour discrimination, les recours efficaces comprennent des procédures judiciaires et administratives garantissant l'accès à la réintégration, à une indemnisation et à des sanctions exécutoires, les inspections du travail jouant un rôle clé dans l'application de ces mesures⁴²¹. Ces recours doivent être adéquats, proportionnés et dissuasifs pour garantir une protection efficace contre la discrimination⁴²².

216. Les systèmes d'IA sont de plus en plus utilisés dans les processus de recrutement⁴²³, ce qui peut avoir des conséquences négatives, par exemple lorsque le recours à l'apprentissage automatique pour l'identification des candidats a abouti à des résultats discriminatoires, ou lorsque des systèmes de reconnaissance faciale et d'analyse des émotions basés sur l'IA ont donné lieu à une discrimination raciale⁴²⁴. À ce titre, les systèmes d'IA utilisés pour le recrutement et la sélection des candidats devraient être objectifs, neutres et exempts de préjugés, y compris de préjugés sexistes. Dans un contexte plus large, les États devraient veiller à ce que l'utilisation de systèmes d'IA sur le lieu de travail ne reproduise pas ou n'amplifie pas les schémas d'inégalité existants et promeuve l'égalité, y compris l'égalité de genre, la diversité et l'inclusion. En particulier, cela pourrait consister en un audit régulier des résultats de l'utilisation des systèmes d'IA dans les procédures de recrutement, de promotion et autres ; l'implication des employés et de leurs organisations représentatives dans les politiques ou les choix concernant l'utilisation de l'IA dans la prise de décision sur le lieu de travail ; le suivi de l'impact de l'introduction des systèmes d'IA dans le lieu de travail sur l'égalité de genre et la diversité au sein de la main-d'œuvre ; et la formation et la sensibilisation de la main-d'œuvre aux préjugés sur les données, aux stéréotypes et aux risques de discrimination lors de l'utilisation des systèmes d'IA.

217. L'utilisation de l'IA dans le domaine de l'emploi comporte également le risque que les inégalités persistent et s'aggravent si, par exemple, les personnes âgées, les personnes en situation de handicap ou les personnes ayant des compétences numériques limitées ne disposent pas des capacités nécessaires pour les utiliser. Pour ces personnes, les

⁴²⁰ Conclusions 2020, Albanie.

⁴²¹ Conclusions 2020, Chypre.

⁴²² Conclusions XVIII-I (2006), Autriche.

⁴²³ Résolution 2343 (2020) Prévenir les discriminations résultant de l'utilisation de l'intelligence artificielle, paragraphe 1. Voir également la Recommandation CM/Rec(2020)1 sur les impacts des systèmes algorithmiques sur les droits de l'homme, paragraphe 8.

⁴²⁴ Étude CDADI/GEC (2023), pp. 19-21.

chances de participer au marché du travail peuvent s'amenuiser. En outre, un accès limité aux systèmes et outils d'IA peut empêcher les individus de profiter des avantages et des bénéfices qu'ils peuvent offrir. Les décideurs politiques devraient veiller à ce que les systèmes d'IA soient accessibles et promouvoir, en collaboration avec les employeurs, le développement et la diffusion de systèmes d'IA qui contribuent à une meilleure participation à l'emploi, tels que les systèmes d'assistance.

Transparence et responsabilité

218. L'utilisation de l'IA dans le domaine du travail et de l'emploi pose des problèmes de transparence et de responsabilité, en particulier dans le contexte de l'embauche, de la détermination des salaires, de la surveillance du lieu de travail et des processus décisionnels. Par exemple, en raison du problème de la boîte noire des systèmes d'IA, la fixation des salaires et l'attribution des tâches dans les plateformes et le gig work peuvent laisser les travailleurs sans explications sur les fluctuations de salaire ou la disponibilité de l'emploi. Les mécanismes de responsabilisation sont tout aussi essentiels pour éviter que l'utilisation de l'IA sur le lieu de travail ne porte atteinte aux droits du travail. Les employeurs et les décideurs politiques devraient mettre en œuvre des réglementations claires, en veillant à ce que les systèmes d'IA s'alignent sur les normes d'équité, de non-discrimination et de protection des travailleurs. Les détenteurs de droits doivent pouvoir disposer de recours efficaces.

Liberté d'expression ; liberté de réunion et d'association

219. L'article 10 de la CEDH (liberté d'expression) s'applique dans le contexte des relations de travail, y compris lorsque celles-ci sont régies par les règles du droit privé ; l'État a l'obligation positive de protéger le droit à la liberté d'expression, même dans le domaine des relations entre particuliers⁴²⁵. L'article 11 de la CEDH (liberté de réunion et d'association) protège à la fois les travailleurs et les syndicats. Un employé ou un travailleur doit être libre d'adhérer ou non à un syndicat sans être sanctionné ou découragé⁴²⁶. Compte tenu du caractère sensible des questions sociales et politiques liées à la recherche d'un juste équilibre entre les intérêts respectifs des travailleurs et des employeurs, et du degré élevé de divergence entre les systèmes nationaux dans ce domaine, les États disposent d'une large marge d'appréciation quant à la manière

⁴²⁵ *Herbai c. Hongrie*, n° 11608/15, 5 novembre 2019, paragraphe 37 ; *Fuentes Bobo c. Espagne*, n° 39293/98, 29 février 2000, paragraphe 38.

⁴²⁶ *Associated Society of Locomotive Engineers and Firemen (ASLEF) c. Royaume-Uni*, n° 11002/05, 27 février 2007, paragraphe 39.

d'assurer la liberté syndicale et la protection des intérêts professionnels des membres des syndicats⁴²⁷.

220. La CSE protège la liberté d'association en tant que droit d'organisation en vertu de l'article 5, garantissant aux travailleurs le droit de former des syndicats et des organisations d'employeurs et de s'y affilier sans autorisation préalable⁴²⁸. L'article 28 de la CSE complète ces protections en sauvegardant l'indépendance des syndicats et en garantissant la protection des représentants des travailleurs⁴²⁹, y compris la protection contre le licenciement ou tout traitement de représailles⁴³⁰ tel que le refus d'avantages sociaux, de formation, de promotions ou les licenciements discriminatoires⁴³¹.

221. La surveillance du lieu de travail par l'IA peut avoir des conséquences négatives sur la liberté d'expression et la syndicalisation. L'utilisation abusive de la surveillance basée sur les systèmes d'IA peut constituer une menace pour la liberté d'expression et la liberté d'association des employés en ayant potentiellement un effet dissuasif sur leurs droits d'avoir des opinions, de recevoir et de transmettre des informations et des idées, de s'organiser, d'organiser des réunions de travailleurs et de communiquer de manière confidentielle. La surveillance des communications, des interactions et des mouvements peut aider les employeurs à réprimer les activités syndicales en entravant les réunions ou en décourageant les employés de s'exprimer. L'absence de protection des salariés contre la discrimination exercée par l'employeur en raison de leurs activités syndicales peut décourager d'autres personnes d'adhérer à ce syndicat, ce qui pourrait conduire à sa disparition⁴³².

222. Afin de prévenir les effets négatifs de la surveillance sur le lieu de travail induite par les systèmes d'IA, les États devraient mettre en place des garanties strictes assurant la transparence, la responsabilité et le respect des articles 10 et 11 de la CEDH et des articles 5 et 28 de la CSE. Les employeurs doivent justifier les mesures de surveillance comme étant nécessaires et proportionnées, avec des limites claires pour éviter les abus antisyndicaux.

⁴²⁷ *Sindicatul "Păstorul cel Bun" c. Roumanie* [GC], n° 2330/09, 9 juillet 2013, paragraphe 133.

⁴²⁸ Conclusions 2010, Géorgie ; Conclusions I (1969), Déclaration d'interprétation de l'article 5.

⁴²⁹ Conclusions 2003, Bulgarie.

⁴³⁰ Conclusions 2018, Fédération de Russie.

⁴³¹ Conclusions 2018, Azerbaïdjan.

⁴³² *Danilenkov et autres c. Russie*, n° 67336/01, 30 juillet 2009, paragraphe 135 ; et *Syndicat de la police de la République slovaque et autres c. Slovaquie*, 25 septembre 2012, n° 11828/08, paragraphes 60-61.

Pour en savoir plus

- CEDH, [*Fiche d'information – Surveillance au travail*](#),
- CEDH, [*Fiche d'information – Droit en matière syndicale*](#)
- CEDH, [*Fiche d'information - Droits relatifs au travail*](#)
- OECD, [*Employment Outlook 2023, Artificial Intelligence and the Labour Market*](#), 2023, en anglais uniquement
- OECD, [*Using AI to Support People with Disability in the Labour Market: Opportunities and Challenges*](#), 2023, en anglais uniquement
- OECD, [*Using AI in the Workplace: Opportunities, Risks and Policy Responses*](#), 2024, en anglais uniquement)
- International Labour Organisation, [*Generative AI and Jobs: A global analysis of potential effects on job quantity and quality*](#), en anglais uniquement
- International Labour Organisation, [*Digital transformation in employment policies*](#), en anglais uniquement
- International Labour Organisation, [*The Algorithmic Management of work and its implications in different contexts*](#), International Labour Organisation, 2022, en anglais uniquement
- McKinsey Global Institute, [*A new future of work: The race to deploy AI and raise skills in Europe and beyond*](#), 2024, en anglais uniquement

Le *Manuel sur les droits humains et l'intelligence artificielle* reflète la contribution du Comité directeur pour les droits humains (CDDH) aux travaux du Conseil de l'Europe sur l'impact de ce qui pourrait bien être l'évolution technologique marquante du XXI^e siècle.

Censé compléter la Convention-cadre du Conseil de l'Europe sur l'intelligence artificielle et les droits de l'homme, la démocratie et l'État de droit, le *Manuel* du CDDH s'appuie sur les principes et les normes des principaux traités du Conseil de l'Europe relatifs aux droits humains, à savoir la Convention européenne des droits de l'homme et la Charte sociale européenne, ainsi que sur les travaux de diverses autres instances du Conseil de l'Europe et d'autres organisations internationales.

Le *Manuel* a été conçu comme un outil accessible destiné principalement à aider les fonctionnaires et les responsables politiques des États membres du Conseil de l'Europe. Afin d'en rendre son usage pratique dans des situations réelles, il fournit des analyses et des conseils sur la manière dont l'utilisation des systèmes de l'IA dans divers secteurs de l'administration publique devrait être examinée sous l'angle des droits humains.

www.coe.int

Le Conseil de l'Europe est la principale organisation de défense des droits humains du continent. Il comprend 46 États membres, dont l'ensemble des membres de l'Union européenne. Tous les États membres du Conseil de l'Europe ont signé la Convention européenne des droits de l'homme, un traité visant à protéger les droits humains, la démocratie et l'État de droit. La Cour européenne des droits de l'homme contrôle la mise en œuvre de la Convention dans les États membres.

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE